

Action1

Software Vulnerability Ratings Report 2024

June 2024

Contents

Introduction	3
Executive Summary	4
Methodology	7
Enterprise Software Categories	9
Software Vulnerability Ratings	10
Vulnerability Analysis and Year-Over-Year Comparison	12
Vulnerability Summary Overview	12
Desktop Operating Systems	15
Mobile Operating Systems	17
Office Apps	19
Remote Management Software	21
Document Viewers	23
Password Managers	25
Antiviruses	27
Image Editors	29
Web Browsers	31
VPN Clients	33
Load Balancers	35
Databases	37
Recommendations	39
Appendix	40

Introduction

This report analyzes the security landscape of enterprise software. Its primary objective is to identify vulnerability trends within commonly used enterprise software categories, with a particular focus on **exploitation rate** and **remote code execution (RCE)** vulnerabilities.

Exploitation rate is the metric developed by the Action1 research team aimed at helping enterprises assess the risks associated with certain vendors' software and the comprehensiveness of their vulnerability management programs.

RCE is a dangerous type of vulnerability as it allows attackers to execute arbitrary code remotely, potentially compromising critical systems. When an application has an increased count of RCE vulnerabilities, it suggests that there are more potential entry points for attackers to exploit the organization's IT environment.

To facilitate trend identification within a representative timeframe, the Action1 research team considered the data from the years 2023, 2022, and 2021.

The report draws insights from two critical sources: the **National Vulnerability Database (NVD)** and **cvedetails.com**. By leveraging NVD data and CVE details, the report quantifies the vulnerabilities, providing a comprehensive view of how the threat landscape changes over time.

Armed with this report, CISOs and CIOs gain strategic insights into their software ecosystem. They can make informed decisions about risk management, resource allocation, and technology investments.

Moreover, CISOs and CIOs can use the report to evaluate software vendors based on their security track record. This informs procurement decisions and strengthens partnerships with security-conscious vendors.

Finally, the report can help organizations be more proactive in risk mitigation as it enables them to focus on critical vulnerabilities, reducing the attack surface and enhancing overall security posture.

Executive Summary

The report provides essential insight into the evolving vulnerability landscape for enterprise software. In light of the current crisis at the National Vulnerability Database (NVD), where new vulnerability uploads have been suspended since May 9, 2024*, this information is invaluable to cybersecurity professionals because it shows the trends for vulnerabilities in popular software, which can help prioritize software for vulnerability monitoring using alternative tools and approaches while the traditional reliance on NVDs is challenged and allocate resources accordingly.

The report highlights a troubling increase in the total number of vulnerabilities across all categories of enterprise software, particularly in the number of exploited vulnerabilities, which increased by 22% in 2023.

The key trends, based on exploitability rates and the dynamics of RCE vulnerabilities within enterprise software categories as well as specific applications, are outlined below.

TREND 1

Load Balancers Are Becoming an Attractive Target with a Record Exploitation Rate.

The trend that catches the eye first is the astonishingly high exploitation rate for NGINX (100%) and Citrix (57%). Vulnerabilities in load balancers pose significant risks, as a single exploit in these systems can provide broad access or disruption capabilities against targeted networks. While the total number of vulnerabilities reported for load balancers over the three-year period analyzed accounts for only 0.2% of the total number of vulnerabilities analyzed, the impact of these severe vulnerabilities, as exemplified by the infamous CitrixBleed, demonstrates that high exploitation rates of vulnerabilities can be more significant indicators than their number.

For organizations, this means they need to pay close attention to ensuring regular updates for the Citrix load balancer or look for alternatives, considering the company's needs.

TREND 2

Apple Operating Systems Are Increasingly Under Attackers' Radar.

Apple operating systems, MacOS and iOS, showed an increased exploitation rate in 2023, 7% and 8% respectively, suggesting that attackers are increasingly exploiting these OS.

Even though MacOS reduced its total vulnerability number by 29%, it reported 30% more exploited vulnerabilities in 2023 than in 2022, totaling 18. While Windows desktop operating systems have the highest number of vulnerabilities, including critical and RCE, their exploitation rates remain stable at 4%, which shows that Microsoft has a stable vulnerability management process with low fluctuation.

MS Windows Server 2016 is the absolute leader in terms of the total number of vulnerabilities. It also reported a record 177 RCEs in 2023. Although Linux reported fewer RCE vulnerabilities in 2023 compared to other operating systems analyzed,

totaling 13, their 63% surge is concerning, especially as it continues a 60% increase from 8 RCEs in 2022. The growth in dangerous RCEs underscores the need for both Windows and Linux researchers to prioritize the discovery and mitigation of this type of vulnerability. For organizations, this highlights the need for proper patching. Nevertheless, our research shows that Linux is the least vulnerable OS to hacker attacks due to the small number of exploited vulnerabilities, which is decreasing further.

In the segment of mobile operating systems, there is an even greater disparity between the total number of vulnerabilities and their exploitation between Google and Apple OS. Specifically, Android reported an absolute record of 1421 vulnerabilities in 2023, with only 3 exploited, resulting in a low exploitation rate of 0.2%. In contrast, while iOS reported 268 vulnerabilities last year, a significant 20 of them were exploited, resulting in a significant exploitation rate of 8%. It's notable that iOS is also the leader in RCE counts over the three years analyzed. These findings underscore the targeted nature of attacks on iOS devices, possibly due to the perception of the valuable data they store.

The increase in exploited vulnerabilities for MacOS and iOS is a concerning trend for Apple. For some reason, the company is not managing to fix vulnerabilities before attackers exploit them. For organizations, this means they should not only ensure regular updates for Apple OS but also consider implementing additional security measures for Mac devices.

Overall, vulnerabilities in operating systems account for around 75% of vulnerabilities analyzed in this research.

The growth in critical RCEs calls for immediate attention from OS vendors, researchers, and organizations.

TREND 3

MSSQL RCE Vulnerabilities Surge 1600%, Highlighting Increased Risk of New Exploits.

In 2023, Microsoft SQL Server (MSSQL) experienced an astonishing 1600% surge in critical vulnerabilities, totaling 17, all of which are RCEs, raising immediate concerns for database administrators and cybersecurity teams. This spike, contrasting with previous years, signals a potential risk that attackers might one day be faster than researchers in discovering and exploiting the next unknown RCE. The current increase in known RCEs suggests to attackers that there might be other undiscovered RCE vulnerabilities in this system.

MSSQL is a lucrative target for hackers due to its widespread use in enterprise environments, housing valuable data like customer information and financial records. Its remote accessibility makes it susceptible to exploitation from anywhere. Consequently, organizations must prioritize robust security measures to safeguard their MSSQL servers and prevent potential data breaches.

MySQL, despite having the highest total number of vulnerabilities over three years, shows promising progress with a 64% decrease in total vulnerabilities in 2023.

MSSQL experienced an astonishing 1600% surge in critical vulnerabilities, totaling 17, all RCEs.

TREND 4

Increased Exploitability of MS Office, Highlighting Attackers' Preferences to Exploit Human Error.

Microsoft Office has the expected highest total number of vulnerabilities among office apps analyzed and a worrying exploitation rate of 7%, an increase from 2% in 2022, illustrating increased threat actors' preference in exploiting user-facing software where human error can be utilized. Additionally, its numerous critical vulnerabilities, accounting for around 80% of the overall vulnerability count annually, with 40%-50% being RCEs, raise significant concerns. This trend suggests we can expect more phishing attacks aimed at exploiting MS Office vulnerabilities.

This underscores the need for CISOs to enforce security awareness among employees and enhance endpoint monitoring with endpoint protection systems, in addition to robust patching.

TREND 5

Spike in RCEs and Exploited Vulnerabilities Raises Concerns about Edge Security.

While Chrome has the highest number of total vulnerabilities over the three-year period analyzed, Edge's record number of 14 RCE vulnerabilities over the same timeframe, which continues to grow, is an alarming insight for us. Specifically, it spiked at 17% in 2023, following a staggering 500% growth in 2022. This trend is concerning for the vendor, despite Edge having a relatively lower total number of vulnerabilities. Overall, the total number of RCEs accounts for 1% for Chrome and Firefox and 10% for Edge. Additionally, Edge reported 4 exploited vulnerabilities in 2023, resulting in a 7% exploitation rate for this web browser – an increase from 2022's 5%.

The fact that Edge faces an increase in RCE and exploited vulnerabilities, despite having a relatively low number of total vulnerabilities, suggests that Microsoft does not yet actively enforce a vulnerability management program for this web browser as rigorously as Google does for Chrome or Mozilla does for Firefox. This implies that it might not be a good idea to use Edge as the main corporate web browser.

Overall, vulnerabilities in web browsers account for around 13% of vulnerabilities analyzed in this research.

*** THE NOTE:**

While [security experts noted a significant drop](#) in enrichment data uploads on the NVD starting February 12, 2024, the above note was made after the enrichment was completely [suspended starting May 9, 2024](#). However, within the next five days, the vulnerability upload process started again, albeit slowly, with months of vulnerability backlog remaining.

Methodology

Data for this research was obtained from NVD and cvedetails.com. The criticality of vulnerabilities was described as follows:

- Critical vulnerabilities have CVSS scores greater than 7.0.
- Moderate vulnerabilities have CVSS scores less than 7.0 but greater than 4.0
- Low severity vulnerabilities have CVSS scores less than 4.0.

Enterprise software categories were defined based on criteria of popularity, criticality in use by organizations, and the total number of vulnerabilities found. Some categories, such as text editors, database management clients, cloud storage apps, and archivers, were excluded due to a lack of a representative number of vulnerabilities in apps within the category, rendering them not relevant to this study.

The criteria used are based on the CISA KEV catalog.

We also kept track of RCE vulnerabilities, which are the most dangerous because they enable remote code execution on a target system via the vulnerable software.

Additionally, the report utilizes the exploitation rate as a metric to demonstrate the ratio of exploited vulnerabilities to the total number of vulnerabilities. The exploitation rate formula** is as follows:

$$\text{Number of exploited vulnerabilities} / \text{total number of vulnerabilities} * 100$$

This metric is valuable because it indicates the software's susceptibility to exploitation, highlighting the diligence of developers in preventing vulnerabilities rather than merely addressing them after they have been exploited by hackers. For example, if the metric is high, meaning that most known vulnerabilities were exploited despite a low total number of vulnerabilities, it can signify a lack of an efficient vulnerability management process in a vendor's organization. Conversely, if the metric is low, even with a high number of exploited vulnerabilities but with a significantly larger total number of vulnerabilities, it can suggest a working vulnerability management process on the vendor's side. The latter scenario could also indicate that the product's code is either lacking in security or highly attractive to threat actors due to its popularity, as seen with Microsoft or Google. If the software has zero exploited vulnerabilities and a large number of total vulnerabilities, it is a sign of a proper patch management process in a vendor's company.

Although the exploitation rate formula alone is not sufficient to evaluate the risks associated with certain software, it can be part of a broader set of metrics to measure a vendor's security performance, especially if combined with other qualitative and quantitative data points.

The data on vulnerabilities for 2021, including their types and exploitation rates, and the data on total vulnerabilities over the three-year period analyzed, are presented in the Appendix.

In the tables with vulnerability data per category year over year, exclamation marks were added to highlight dominating values of vulnerabilities in specific apps, whether by total number or by a specific type of vulnerability.

**** DISCLAIMER:**

- The formula only considers the number of exploited vulnerabilities in relation to the total number of known vulnerabilities. It doesn't take into account the severity of the vulnerabilities, the potential impact of exploitation, the number of exploitation attempts, or the ease of exploitation – criteria that should also be considered when evaluating risks associated with a particular software.
- Not all exploited vulnerabilities are reported, so the numerator in the formula may be underestimated. Similarly, not all vulnerabilities in software may have been discovered or disclosed.
- The timing of the patch release and vulnerability exploitation are other important criteria that are not considered within the formula.

Enterprise Software Categories

<p>Desktop Operating Systems</p> <ul style="list-style-type: none"> ▪ MS Windows 10 ▪ MS Windows Server 2016 ▪ MacOS ▪ Linux 	<p>Mobile Operating Systems</p> <ul style="list-style-type: none"> ▪ iOS ▪ Android ▪ HarmonyOs 	<p>Office Apps</p> <ul style="list-style-type: none"> ▪ Microsoft Office ▪ Libre Office ▪ Open Office
<p>Remote Management Software</p> <ul style="list-style-type: none"> ▪ TeamViewer ▪ DameWare ▪ Splashtop ▪ AnyDesk ▪ RealVNC 	<p>Document Viewers</p> <ul style="list-style-type: none"> ▪ Adobe Reader ▪ Foxit Reader ▪ Nitro PDF 	<p>Password Manager Clients</p> <ul style="list-style-type: none"> ▪ Keepass ▪ Keepass XC ▪ 1Password ▪ Bitwarden ▪ LastPass
<p>Antiviruses</p> <ul style="list-style-type: none"> ▪ Avast ▪ Bitdefender ▪ Malwarebytes ▪ ESET ▪ Kaspersky ▪ McAfee 	<p>Image Editors</p> <ul style="list-style-type: none"> ▪ Adobe Photoshop ▪ Gimp ▪ Paint.Net ▪ Adobe Illustrator 	<p>VPN Clients</p> <ul style="list-style-type: none"> ▪ Cisco Any Connect ▪ FortiClient ▪ OpenVPN ▪ WireGuard
<p>Web Browsers</p> <ul style="list-style-type: none"> ▪ Chrome ▪ Firefox ▪ Edge 	<p>Load Balancers</p> <ul style="list-style-type: none"> ▪ HaProxy ▪ Citrix ▪ NGINX 	<p>Databases</p> <ul style="list-style-type: none"> ▪ MSSQL ▪ Mysql ▪ Oracle ▪ Postgresql

Software Vulnerability Ratings

TABLE 1. TOP EXPLOITED SOFTWARE IN 2023 VS. 2022.

Name	Exploitation Rate 2023	Exploitation Rate 2022
NGINX	100% NEW	0
Citrix	57% NEW	0
iOS	8% ↑	4%
Microsoft Office	7% ↑	2%
MacOS	7% ↑	3%
Edge	7% ↑	5%
MS Windows Server 2016	4%	4%
MS Windows 10	4%	4%
Firefox	3% ↓	4%
Adobe Reader	2% ↑	0

In 2023, the software analyzed in this research exhibited the highest exploitation rates compared to other years under review, indicating an intensified threat landscape. The table above showcases the ratings of the software applications with the highest exploitation rates in 2023, along with their rates back in 2022, enabling us to observe any changes where applicable. The software marked as 'New' indicates that these applications appeared for the first time during the three-year period analyzed (meaning they reported exploited vulnerabilities in 2023 only). This highlights the emergence of a new trend among hackers in exploiting perimeter software, specifically load balancers.

What immediately draws attention is NGINX's 100% exploitation rate. Notably, this high percentage is attributed to a single reported vulnerability that was exploited. Interestingly, this scenario is exceptional; we didn't observe it with any of the 47 software applications presented in this research report. *** These findings suggest that NGINX may lack sufficient vulnerability management and remediation processes and might even be prone to other vulnerabilities which were not disclosed. Overall, it seems that NGINX should pay attention to its vulnerability management program.

Another significant finding is Citrix with an exploitation rate of 57%, which experienced several exploited vulnerabilities under the name CitrixBleed.

Additionally, there are unusually high exploitation rates for iOS, Microsoft Office, MacOS, and Microsoft Edge in 2023, all showing a significant increase from 2022.

A concerning trend of the growth in exploitation rates may continue in 2024.

Note: The exploitation rate values here and in the main part of the report have been rounded for ease of visual perception and clarity. Detailed values with decimal places are provided in the Appendix.

*** None of the 62 analyzed applications reported in total only one vulnerability that was exploited. (We excluded detailed analysis on 15 applications from the research report due to the low significance of the findings.)

Vulnerability Analysis and Year-Over-Year Comparison

Vulnerability Summary Overview

The report reveals a concerning trend for cybersecurity specialists: the overall number of vulnerabilities has increased from 2021 to 2023 across software categories analyzed, as well as the number of exploited and RCE vulnerabilities.

TABLE 2. TOTAL VULNERABILITIES, EXPLOITED, RCE, BY YEAR

	2021	2022	2023
All Vulnerabilities	3942	4449	4359
RCE	519	536	540
Exploited	74	88	107

For many categories, the number of critical vulnerabilities remains high or increased since 2021, underscoring the constant intensity of the threat landscape and the need for prioritized patch management. The trend of critical vulnerabilities outnumbering medium vulnerabilities is seen in 10 out of 12 groups.

TABLE 3. TOTAL CRITICAL VS. TOTAL MEDIUM BY CATEGORY

Category Name	Total Critical 2021-2023	Total Medium 2021-2023
Desktop Operating Systems	3393	1435
Mobile Operating Systems	2188	2390
Office Apps	226	51
Remote Management Software	12	4
Document Viewers	270	148
Password Manager Clients	4	8
Antivirus	61	25
Image Editors	86	44
Video Editors	39	16
Web Browsers	1024	624
VPN Clients	42	17
Load Balancers	25	5
Databases	37	263

Desktop operating systems and mobile operating systems have a significantly higher number of reported vulnerabilities compared to other groups, accounting for 75% of all vulnerabilities examined in our research. This proportion underscores that operating systems are a consistent target area for attackers due to their widespread use and critical role in IT infrastructures.

TABLE 4. TOTAL VULNERABILITIES BY CATEGORY

Category Name	Total Vulnerabilities 2021-2023	Percentage
Desktop Operating Systems	4885	38.4%
Mobile Operating Systems	4760	37.4%
Office Apps	279	2.2%
Remote Management Software	17	0.1%
Document Viewers	418	3.3%
Password Manager Clients	12	0.1%
Antivirus	86	0.7%
Image Editors	130	1.0%
Video Editors	57	0.4%
Web Browsers	1655	13.0%
VPN Clients	60	0.5%
Load Balancers	30	0.2%
Databases	322	2.5%
Total	12711	

Desktop Operating Systems

TABLE 5. DESKTOP OS VULNERABILITIES 2023 ANALYSIS

Name	All Vulnerabilities 2023	YoY 2023-2022	Critical 2023	YoY 2023-2022	Medium 2023	YoY 2023-2022	Low 2023	YoY 2023-2022	RCE 2023	YoY 2023-2022	Exploited 2023	YoY 2023-2022
Desktop Operating Systems	1562	-9%	1033	-15%	504	5%	25	47%	396	1%	56	0%
MS Windows 10	⚠️ 489	-6%	388	-8%	101	1%	0	-100%	156 ▲	8%	17	-15%
MS Windows Server 2016	⚠️ 501	-3%	390	-6%	111	12%	0	-100%	177 ▲	13%	18	0%
MacOS	▼ 260	-29%	113 ▼	-53%	126	6%	21	200%	50	-39%	18 ▲	50%
Linux	312	1%	142	1%	166	2%	4	-50%	13 ▲	63%	3	-50%

TABLE 6. DESKTOP OS VULNERABILITIES 2022 ANALYSIS

Name	All Vulnerabilities 2022	YoY 2023-2022	Critical 2022	YoY 2023-2022	Medium 2022	YoY 2023-2022	Low 2022	YoY 2023-2022	RCE 2022	YoY 2023-2022	Exploited 2022	YoY 2023-2022
Desktop Operating Systems	1709	6%	1212	6%	480	6%	17	13%	391	27%	56	30%
MS Windows 10	⚠️ 521	7%	420	11%	100	-7%	1	0%	144 ▲	25%	20 ▲	33%
MS Windows Server 2016	⚠️ 514	2%	414	6%	99	-12%	1	0%	157 ▲	25%	18 ▲	13%
MacOS	▼ 364	-21%	238 ▼	-20%	119	-25%	7	40%	82	30%	12	0%
Linux	310	91%	140	75%	162	119%	8	0%	8 ▲	60%	6	0

Key Takeaways:

- The number of RCE vulnerabilities has been steadily increasing for Windows and Linux for two years in a row. Specifically, in Windows Server 2016, the number of RCE vulnerabilities increased by 13% in 2023, totaling 177, and by 25% in 2022, totaling 157. In Windows 10, the number of RCE vulnerabilities increased by 8% in 2023, totaling 156, and by 25% in 2022, totaling 144. Linux reports a smaller total number of RCE vulnerabilities in 2023, totaling 13, but its 63% surge is concerning, especially as it continues a 60% surge from 8 RCEs in 2022. This negative trend suggests a need to closely monitor developments in Linux operating systems in 2024.
- Apple has reduced its total number of vulnerabilities steadily, by 29% in 2023, and by 21% in 2022. Additionally, it reduced the number of critical vulnerabilities in MacOS by an astonishing 62% over 2021-2023. However, it reported a significant number of exploited vulnerabilities in 2023, resulting in a significant exploitation rate of 7%, which suggests that MacOS may be increasingly vulnerable to attacks that exploit known vulnerabilities.
- From 2021 to 2023, MS Windows Server 2016 reported the highest total number of vulnerabilities, totaling 1518. Additionally, it recorded the highest number of critical vulnerabilities during the same period, with 1194 reported. In contrast, Linux reported the smallest number of vulnerabilities over the same period, with only 784.
- While Windows operating systems have many vulnerabilities, including critical and RCE, their exploitation rates have not deteriorated, suggesting improved security responses. Every year, there is a stable 3-4% exploitation rate, which shows that Microsoft has a stable vulnerability management process with low fluctuation.
- Linux is the least vulnerable OS to hacker attacks due to the small number of exploited vulnerabilities, which is decreasing further.

OTHER TAKEAWAYS:

The total number of vulnerabilities reported for operating systems in 2023 was 1562, which represents a downward trend from the 1709 vulnerabilities reported in 2022 and even from the 1614 vulnerabilities reported in 2021. Microsoft's trend is stable – it reports around 500 vulnerabilities per year.

Another interesting finding is that the numbers of vulnerabilities reported for MS Windows 10 and MS Windows Server 2016 are very similar, even though they are two different versions of the same operating system. This suggests that the underlying code base for these versions may have similar vulnerabilities. It's interesting to note that while MacOS may not have as many critical vulnerabilities as some other operating systems, it still has a significant number of vulnerabilities that could harm the system – specifically, it has a high number of medium severity vulnerabilities, with 403 reported in 2021-2023.

It's also notable that the number of exploited vulnerabilities reported for Windows systems and MacOS is very similar – for example, in 2023 Windows 2016 and MacOS reported 18, and MS Windows 10 – 17, which challenges common perceptions about their security.

In 2022 and 2023, Linux leads in terms of the number of medium-severity vulnerabilities. Additionally, while the number of critical vulnerabilities is generally lower than in other operating systems analyzed, it increases every year. Although its RCE and exploitation rates remain significantly lower, underscoring its strength in certain aspects of security, the overall trend of growing vulnerabilities could affect its reputation if it continues.

Our analysis underscores the continuing evolution of threats and the need for proactive security strategies across all operating systems.

Mobile Operating Systems

TABLE 7. MOBILE OS VULNERABILITIES 2023 ANALYSIS

Name	All Vulnerabilities 2023	YoY 2023-2022	Critical 2023	YoY 2023-2022	Medium 2023	YoY 2023-2022	Low 2023	YoY 2023-2022	RCE 2023	YoY 2023-2022	Exploited 2023	YoY 2023-2022
Mobile Operating Systems	1883	9%	685	-21%	1152	51%	46	-54%	67	-25%	23	109%
iOS	268	10%	121	-22%	122	54%	25	178%	⚠️ 43	-40%	⚠️ 20 ▲	100%
Android	⚠️ 1421	16%	401	-19%	1001	54%	19	-77%	24	41%	3	200%
HarmonyOs	194	-25%	163	-23%	29	-15%	2	-80%	0	N/A	0	N/A

TABLE 8. MOBILE OS VULNERABILITIES 2022 ANALYSIS

Name	All Vulnerabilities 2022	YoY 2022-2021	Critical 2022	YoY 2022-2021	Medium 2022	YoY 2022-2021	Low 2022	YoY 2022-2021	RCE 2022	YoY 2022-2021	Exploited 2022	YoY 2022-2021
Mobile Operating Systems	1723	49%	862	34%	761	60%	100	178%	89	31%	11	-21%
iOS	243	-36%	155	-35%	79	-40%	9	-18%	⚠️ 72 ▲	85%	⚠️ 10	-29%
Android	⚠️ 1223	86%	494	55%	648	104%	81	286%	17	-39%	1	N/A
HarmonyOs	257	118%	213	148%	34	21%	10	150%	0	-100%	0	N/A

Although iOS shows a decrease in total vulnerabilities from 2021 to 2023, it is the leader in total RCE count over the three years analyzed. Additionally, it has a 100% increase in the number of exploited vulnerabilities in 2023, resulting in 20 exploited vulnerabilities and an exploitation rate of 8%, highlighting the growing targeted nature of attacks, possibly due to the perception of valuable data stored on iOS devices.

The top RCE count and high exploitation rate highlight the growing targeted nature of attacks against iOS devices.

Despite a negative trend showing steady growth in vulnerabilities, totaling the absolute record summary of 3,300 vulnerabilities, Android only reported 69 RCE vulnerabilities and 4 instances of exploitation over the past three years within our research, resulting in a low exploitation rate of 0.2% in 2023, 0.1% in 2022, and 0% in 2021. A low rate of exploitation and low number of RCE vulnerabilities suggest potential resilience against sophisticated threats. Additionally, this discovery challenges the prevailing perception of Android's susceptibility to attacks. Despite its expansive attack surface, potentially attributable to its open-source nature and higher market share, the low number of exploited vulnerabilities suggests either the implementation of effective mitigation strategies or a reduced interest from attackers in exploiting these vulnerabilities.

Android's low exploitation rate and RCE vulnerabilities number suggest potential resilience against high-level threats.

HarmonyOS, with its high rate of critical vulnerabilities but minimal RCE and exploitation instances, presents a unique security profile that warrants close observation as it continues to grow. At the same time, HarmonyOS's high percentage of critical vulnerabilities, despite its lower total number, suggests that the vulnerabilities affecting it may be more severe on average - a critical insight for users and developers.

Overall, mobile operating systems saw an increase from 1154 vulnerabilities in 2021 to 1883 in 2023, highlighting the growing importance of mobile security.

Office Apps

TABLE 9. OFFICE APPS 2023 VULNERABILITIES ANALYSIS

Name	All Vulnerabilities 2023	YoY 2023-2022	Critical 2023	YoY 2023-2022	Medium 2023	YoY 2023-2022	Low 2023	YoY 2023-2022	RCE 2023	YoY 2023-2022	Exploited 2023	YoY 2023-2022
Office Apps	93	31%	78	59%	14	-33%	1	0%	32	14%	6	500%
Microsoft Office	⚠️ 85 ▲	33%	⚠️ 72 ▲	67%	12	-40%	1	0%	⚠️ 32 ▲	19%	6 ▲	500%
Libre Office	5	0%	3	-25%	2	100%	0	N/A	0	-100%	0	N/A
Open Office	3	50%	3	50%	0	N/A	0	N/A	0	N/A	0	N/A

TABLE 10. OFFICE APPS 2022 VULNERABILITIES ANALYSIS

Name	All Vulnerabilities 2022	YoY 2022-2021	Critical 2022	YoY 2022-2021	Medium 2022	YoY 2022-2021	Low 2022	YoY 2022-2021	RCE 2022	YoY 2022-2021	Exploited 2022	YoY 2022-2021
Office Apps	71	-38%	49	-51%	21	31%	1	N/A	28	-44%	1	-86%
Microsoft Office	⚠️ 64	-38%	⚠️ 43	-53%	20	54%	1	N/A	⚠️ 27	-46%	1	-86%
Libre Office	5	25%	4	33%	1	0%	0	N/A	1	N/A	0	N/A
Open Office	2	-71%	2	-60%	0		0	N/A	0	N/A	0	N/A

In 2023, Microsoft Office showed a significant exploitation rate of 7%, which decreased from 2% in 2022 (in 2021, it was 7%, too). This illustrates its attractiveness to threat actors and reflects attackers' preference for exploiting user-facing software where human error can often be utilized. Microsoft Office's numerous critical vulnerabilities, accounting for around 80% of the overall vulnerability amount annually, with roughly 40%-50% being RCEs, along with numerous exploited vulnerabilities, raise growing concerns.

MS Office's growing number of critical, RCE, and exploited vulnerabilities illustrates its increased attractiveness to threat actors.

Specifically, in 2023, the total number of vulnerabilities in Microsoft Office increased by 33%, critical vulnerabilities by an astonishing 67%, RCE vulnerabilities by 19%, and exploited vulnerabilities by 500%. Of the 85 vulnerabilities detected, 72 were critical, and 32 were RCE-related. Microsoft Office is the only application among the three with 6 exploited vulnerabilities, totaling 14 over the period analyzed. This illustrates that Microsoft Office, with its large user base and integral role in organizations' operations, is a preferred tool for hackers in phishing campaigns. They lure users with "important" documents containing malicious code that facilitates control over the victim's system.

OpenOffice has the lowest total number of vulnerabilities among the three, which could be interpreted as it being the safer option or as it being a less audited/tested product. OpenOffice

saw a decrease in the total number of reported vulnerabilities from 2021 to 2023.

Both LibreOffice and OpenOffice did not have any vulnerabilities exploited over the analyzed period. The low vulnerability numbers by LibreOffice and OpenOffice suggest less focus from attackers and security researchers. We do not believe that they benefit from their open-source nature in terms of faster vulnerability identification and remediation.

Remote Management Software

TABLE 11. REMOTE MANAGEMENT SOFTWARE 2023 VULNERABILITIES ANALYSIS

Name	All Vulnerabilities 2023	YoY 2023-2022	Critical 2023	YoY 2023-2022	Medium 2023	YoY 2023-2022	Low 2023	YoY 2023-2022	RCE 2023	YoY 2023-2022	Exploited 2023	YoY 2023-2022
Remote Management Software	2	-67%	1	-75%	1	0%	0	-100%	0	-100%	0	N/A
TeamViewer	1	-67%	0	-100%	1	0%	0	-100%	0	-100%	0	N/A
DameWare	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A
Splashtop	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A
AnyDesk	1	0%	1	0%	0	N/A	0	N/A	0	N/A	0	N/A
RealVNC	0	-100%	0	-100%	0	N/A	0	N/A	0	N/A	0	N/A

TABLE 12. REMOTE MANAGEMENT SOFTWARE 2022 VULNERABILITIES ANALYSIS

Name	All Vulnerabilities 2022	YoY 2022-2021	Critical 2022	YoY 2022-2021	Medium 2022	YoY 2022-2021	Low 2022	YoY 2022-2021	RCE 2022	YoY 2022-2021	Exploited 2022	YoY 2022-2021
Remote Management Software	6	-33%	4	-43%	1	-50%	1	N/A	2	100%	0	N/A
TeamViewer	3	50%	1	-50%	1	N/A	1	N/A	2	100%	0	N/A
DameWare	0	-100%	0	-100%	0	N/A	0	N/A	0	N/A	0	N/A
Splashtop	0	-100%	0	-100%	0	N/A	0	N/A	0	N/A	0	N/A
AnyDesk	1	-67%	1	-50%	0	N/A	0	N/A	0	N/A	0	N/A
RealVNC	2	100%	2	N/A	0	N/A	0	N/A	0	N/A	0	N/A

The data indicates a positive trend in the decreasing number of vulnerabilities in remote management software over the analyzed period, particularly in the reduction of RCE and total vulnerabilities. This is significant, considering that such software has always been targeted by hackers. Specifically, the three vendors analyzed reported only 2 vulnerabilities in 2023, 6 in 2022, and 9 in 2021. Although TeamViewer reported 2 RCEs in 2022 and 1 in 2021, it reversed this trend to 0 in 2023. No other vendor reported RCEs during the analyzed period.

The absence of reported exploited vulnerabilities suggests that effective mitigation strategies are in place.

The trend of critical vulnerabilities is also decreasing, which is promising. The highest number of critical vulnerabilities was found in AnyDesk - 4, second is TeamViewer with 3, third place is split between RealVNC and Splashtop - 2.

AnyDesk stands out for having 1 critical vulnerability out of a total of 5 in 2023, highlighting the need for continued vigilance even in years when fewer vulnerabilities are reported overall.

Document Viewers

TABLE 13. DOCUMENT VIEWERS 2023 VULNERABILITIES ANALYSIS

Name	All Vulnerabilities 2023	YoY 2023-2022	Critical 2023	YoY 2023-2022	Medium 2023	YoY 2023-2022	Low 2023	YoY 2023-2022	RCE 2023	YoY 2023-2022	Exploited 2023	YoY 2023-2022
Document Viewers	98	-23%	64	-14%	34	-36%	0	N/A	4	-60%	2	N/A
Adobe Reader	! 92 ▼	-27%	58	-21%	34	-36%	0	N/A	3 ▼	-70%	2	N/A
Foxit Reader	6 ▲	500%	6 ▲	500%	0	N/A	0	N/A	1	N/A	0	N/A
Nitro PDF	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A

TABLE 14. DOCUMENT VIEWERS 2022 VULNERABILITIES ANALYSIS

Name	All Vulnerabilities 2022	YoY 2022-2021	Critical 2022	YoY 2022-2021	Medium 2022	YoY 2022-2021	Low 2022	YoY 2022-2021	RCE 2022	YoY 2022-2021	Exploited 2022	YoY 2022-2021
Document Viewers	127	-34%	74	-44%	53	-13%	0	N/A	10	-84%	0	-100%
Adobe Reader	! 126 ▲	37%	73	26%	53	56%	0	N/A	! 10 ▲	900%	0	-100%
Foxit Reader	1 ▼	-99%	1 ▼	-99%	0		0	N/A	0	-100%	0	N/A
Nitro PDF	0	-100%	0	-100%	0	N/A	0	N/A	0	N/A	0	N/A

The number of RCE vulnerabilities reported for PDF viewers is generally decreasing over the period analyzed, suggesting improved security measures. In 2021, Foxit Reader reported an astonishing 63 RCE vulnerabilities, and Adobe – 1; in 2022, Foxit Reader disclosed 0 RCEs, and Adobe Reader – 10; in 2023, Foxit Reader showed 1 RCE, and Adobe Reader – 3.

Adobe Reader is the most targeted PDF viewer analyzed, accounting for 74% of all vulnerabilities in the category, stressing the need for proactive vulnerability management and updates. Notably, it is also the only PDF viewer to exhibit 2 exploited vulnerabilities in 2023 and 1 in 2021. Adobe Reader has consistently reported a high number of vulnerabilities over the years, with a total of 310 vulnerabilities, a significant portion of which are critical (58 of 92 in 2023 and 73 of 126 in 2022).

Nitro PDF had the fewest vulnerabilities among the three, with only 3 reported in 2021 and none in the subsequent two years. This could indicate a smaller user base, making it a less attractive target, or less thorough vulnerability detection and reporting mechanisms.

The number of RCE vulnerabilities reported for PDF viewers is decreasing.

An unusual trend observed in Foxit PDF Reader, which reduced the number of vulnerabilities from 98 in 2021 to 1 in 2022 and 6 in 2023, representing a more than 90% decrease – quite unbelievable. Additionally, 71 of its 98 vulnerabilities disclosed in 2021 were rated as critical, and 63 – as RCEs. The sharp drop in reported vulnerabilities in subsequent years may indicate an aggressive response to this issue or some serious changes in their vulnerability management program. Nevertheless, it's possible that we may see a spike in vulnerabilities in 2024, so it's something to keep an eye on.

Password Managers

TABLE 15. PASSWORD MANAGERS 2023 VULNERABILITIES ANALYSIS

Name	All Vulnerabilities 2023	YoY 2023-2022	Critical 2023	YoY 2023-2022	Medium 2023	YoY 2023-2022	Low 2023	YoY 2023-2022	RCE 2023	YoY 2023-2022	Exploited 2023	YoY 2023-2022
Password Manager Clients	6	100%	3	200%	3	50%	0	N/A	0	N/A	0	N/A
Keepass	2	100%	1	0%	1	N/A	0	N/A	0	N/A	0	N/A
Keepass XC	1	N/A	0	N/A	1	N/A	0	N/A	0	N/A	0	N/A
1Password	0	-100%	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A
Bitwarden	3	N/A	2	N/A	1	N/A	0	N/A	0	N/A	0	N/A
LastPass	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A

TABLE 16. PASSWORD MANAGERS 2022 VULNERABILITIES ANALYSIS

Name	All Vulnerabilities 2022	YoY 2022-2021	Critical 2022	YoY 2022-2021	Medium 2022	YoY 2022-2021	Low 2022	YoY 2022-2021	RCE 2022	YoY 2022-2021	Exploited 2022	YoY 2022-2021
Password Manager Clients	3	0%	1	N/A	2	-33%	0	N/A	0	-100%	0	N/A
Keepass	1	N/A	1	N/A	0	N/A	0	N/A	0	N/A	0	N/A
Keepass XC	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A
1Password	2	-33%	0	N/A	2	-33%	0	N/A	0	-100%	0	N/A
Bitwarden	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A
LastPass	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A

Password manager vendors are grappling with the growing number of vulnerabilities in their products, likely due to the increasing popularity of password managers among regular users. The total number of vulnerabilities reported for password managers in 2023 was 6, which marks a significant increase from the 3 vulnerabilities reported in 2022 and the 3 vulnerabilities reported in 2021.

Keepass XC has the fewest number of vulnerabilities among the analyzed password managers, with the sole vulnerability appearing in 2023.

Keepass reports only 3 vulnerabilities over three years, with a slight increase noted in 2023.

While LastPass reported no vulnerabilities across the years analyzed, its 2022 breach suggests that its security is not impervious, and it may be susceptible to older vulnerabilities.

1Password has encountered 5 vulnerabilities over the three-year period, with a downward trend observed in 2023.

Bitwarden reported only 3 vulnerabilities in 2023. The sudden increase in Bitwarden's vulnerabilities in 2023, following years with none reported, may prompt questions regarding newly introduced features, heightened scrutiny due to growing popularity, or changes in their vulnerability assessment processes.

LastPass stands out for having no reported vulnerabilities across all years, which could indicate either an excellent security posture or potentially underreported/undiscovered vulnerabilities. However, the breach in 2022 suggests that LastPass' security is not impervious and that it may be susceptible to older vulnerabilities. Though their reporting dates extend beyond this research, these vulnerabilities could still do harm. Thus, it is advisable to monitor this software closely for any emerging vulnerabilities.

Antiviruses

TABLE 17. ANTIVIRUSES 2023 VULNERABILITIES ANALYSIS

Name	All Vulnerabilities 2023	YoY 2023-2022	Critical 2023	YoY 2023-2022	Medium 2023	YoY 2023-2022	Low 2023	YoY 2023-2022	RCE 2023	YoY 2023-2022	Exploited 2023	YoY 2023-2022
Antivirus	21	5%	14	-13%	7	75%	0	N/A	0	-100%	0	N/A
Avast	6	50%	4	33%	2	100%	0	N/A	0	-100%	0	N/A
Bitdefender	2	-67%	2	-60%	0	N/A	0	N/A	0	N/A	0	N/A
Malwarebytes	6	500%	5	400%	1	N/A	0	N/A	0	N/A	0	N/A
Eset	3	-40%	3	-25%	0	N/A	0	N/A	0	N/A	0	N/A
Kaspersky	0	-100%	0	-100%	0	N/A	0	N/A	0	-100%	0	N/A
McAfee	4	300%	0	-100%	4	N/A	0	N/A	0	-100%	0	N/A

TABLE 18. ANTIVIRUSES 2022 VULNERABILITIES ANALYSIS

Name	All Vulnerabilities 2022	YoY 2022-2021	Critical 2022	YoY 2022-2021	Medium 2022	YoY 2022-2021	Low 2022	YoY 2022-2021	RCE 2022	YoY 2022-2021	Exploited 2022	YoY 2022-2021
Antivirus	20	-56%	16	-48%	4	-71%	0	N/A	3	-25%	0	-100%
Avast	4	-43%	3	-50%	1	0%	0	N/A	1	N/A	0	N/A
Bitdefender	6	-57%	5	-50%	1	-75%	0	N/A	0	-100%	0	N/A
Malwarebytes	1	0%	1	0%	0	N/A	0	N/A	0	N/A	0	N/A
Eset	5	150%	4	N/A	1	-50%	0	N/A	0	N/A	0	N/A
Kaspersky	3	-63%	2	-60%	1	-67%	0	N/A	1	N/A	0	N/A
McAfee	1	-92%	1	-89%	0	N/A	0	N/A	1	0%	0	-100%

Bitdefender and Kaspersky show a steadily decreasing trend in vulnerabilities over the three-year period, while others fluctuate. Interestingly, Bitdefender has decreased the number of its critical vulnerabilities by 67% in 2023, and by 57% in 2022. This steady decrease suggests that the potential impact of these vulnerabilities was significant enough for the company to improve its critical vulnerability remediation strategies. Avast and Malwarebytes stand out with 6 total vulnerabilities reported in 2023, showing a 50% and 500% YoY increase respectively.

RCE vulnerabilities have been identified in Bitdefender, Kaspersky, and McAfee over the three-year period, with Bitdefender having the most (3). Since RCEs can allow attackers to run arbitrary code on victim machines, their presence is concerning despite the low numbers. The lack of widespread exploitation of these vulnerabilities may indicate that antivirus vendors are generally quick to patch them, or that these vulnerabilities are not easily exploitable. At the same time, the presence of a single exploited vulnerability in McAfee back in 2021 demonstrates that risks to end users can materialize.

While there are variations in the number and severity of vulnerabilities across antivirus vendors, the overall trend suggests security improvements.

Image Editors

TABLE 19. IMAGE EDITORS 2023 VULNERABILITIES ANALYSIS

Name	All Vulnerabilities 2023	YoY 2023-2022	Critical 2023	YoY 2023-2022	Medium 2023	YoY 2023-2022	Low 2023	YoY 2023-2022	RCE 2023	YoY 2023-2022	Exploited 2023	YoY 2023-2022
Image Editors	32	-52%	23	-36%	9	-71%	0	N/A	1	-80%	0	N/A
Adobe Photoshop	14	-52%	6	-76%	8	100%	0	N/A	0	-100%	0	N/A
Gimp	0	-100%	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A
Paint.Net	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A
Adobe Illustrator	18	-50%	17	55%	1	-96%	0	N/A	1	0%	0	N/A

TABLE 20. IMAGE EDITORS 2022 VULNERABILITIES ANALYSIS

Name	All Vulnerabilities 2022	YoY 2022-2021	Critical 2022	YoY 2022-2021	Medium 2022	YoY 2022-2021	Low 2022	YoY 2022-2021	RCE 2022	YoY 2022-2021	Exploited 2022	YoY 2022-2021
Image Editors	67	116%	36	33%	31	675%	0	N/A	5	150%	0	N/A
Adobe Photoshop	29	93%	25	79%	4	300%	0	N/A	4	N/A	0	N/A
Gimp	2	100%	0	-100%	2	N/A	0	N/A	0	N/A	0	N/A
Paint.Net	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A
Adobe Illustrator	36	140%	11	-8%	25	733%	0	N/A	1	-50%	0	N/A

The analysis reveals a stark contrast in the vulnerability landscape between Adobe and non-Adobe image editors, with Adobe products having more vulnerabilities.

Both Adobe Photoshop and Illustrator have a high number of vulnerabilities, with critical vulnerabilities making up a significant portion. Notably, although there is a 50%-52% decrease in the overall vulnerability number for both Adobe image editors, Illustrator reported 54% more critical vulnerabilities in 2023 than in 2022, indicating increased security risks for this specific editor.

Both Illustrator and Photoshop reported RCE vulnerabilities over 2023-2021, 4 and 4 accordingly, but none of those were actively exploited. This is a positive sign, indicating either a quick response time by vendors to patch vulnerabilities or a lack of interest by attackers in exploiting these vulnerabilities.

Both Illustrator and Photoshop reported RCE vulnerabilities over 2023-2021, but none of those were actively exploited.

However, the trend toward fewer vulnerabilities in Adobe products in 2023 may indicate improved security measures.

Paint.Net stands out with zero reported vulnerabilities over the three years. This could reflect exceptional security measures, low reporting/disclosure rates, or possibly a lower detection rate due to a smaller user base or other factors. The absolute lack of reported vulnerabilities makes Paint.Net remarkably noteworthy.

A fewer number of vulnerabilities in non-Adobe software can indicate better inherent security, less scrutiny by researchers, smaller user base, or simply because these products are open source and not direct competitors to Adobe.

Web Browsers

TABLE 21. WEB BROWSERS 2023 VULNERABILITIES ANALYSIS










Name	All Vulnerabilities 2023	YoY 2023-2022	Critical 2023	YoY 2023-2022	Medium 2023	YoY 2023-2022	Low 2023	YoY 2023-2022	RCE 2023	YoY 2023-2022	Exploited 2023	YoY 2023-2022
Web Browsers	536	-3%	294	-19%	238	29%	4	100%	14	133%	14	-22%
Chrome	296 	-17% 	180	-30%	115	15%	1	N/A	5	N/A	5 	-50%
Firefox	180	15%	87	6%	91	23%	2	100%	2	N/A	5	-17%
Edge	60 	62%	27	8%	32	191%	1	0%	7 	17%	4 	100%

TABLE 22. WEB BROWSERS 2022 VULNERABILITIES ANALYSIS

Name	All Vulnerabilities 2022	YoY 2022-2021	Critical 2022	YoY 2022-2021	Medium 2022	YoY 2022-2021	Low 2022	YoY 2022-2021	RCE 2022	YoY 2022-2021	Exploited 2022	YoY 2022-2021
Web Browsers	551	-3%	364	-1%	185	-8%	2	100%	6	0%	18	157%
Chrome	357	1%	257	3%	100	-3%	0	N/A	0	-100%	10	67%
Firefox	157	17%	82	28%	74	7%	1	0%	0	N/A	6	N/A
Edge	37 	-54%	25	-52%	11	-62%	1	N/A	6 	500%	2 	100%

Unsurprisingly, Chrome has the highest total number of vulnerabilities reported over the three years, with 1,006 vulnerabilities. It leads significantly over Firefox (471 vulnerabilities) and Edge (178 vulnerabilities). This suggests that Chrome's massive codebase and extensive feature set may contribute to a larger attack surface. Additionally, Edge shares the same engine as Chrome, and most Chrome vulnerabilities affect Edge as well.

While Chrome has the highest number of total vulnerabilities over the three-year period analyzed, Edge's record number of 14 RCE vulnerabilities over the same timeframe, which continues to grow, is an alarming insight for us. Specifically, it spiked at 17% in 2023, following a staggering 500% growth in 2022. This trend is concerning for the vendor, despite Edge having a relatively lower total number of vulnerabilities. Overall, the total number of RCEs accounts for 1% for Chrome and Firefox and 10% for Edge.

Edge's record number of 14 RCE vulnerabilities over three years, which continues to grow, is alarming.

Firefox shows a steady increase in critical vulnerabilities, surging by 28% in 2022 and by 6% in 2023, which may necessitate the vendor to strengthen security. The overall number of vulnerabilities is also growing.

While Chrome leads in the number of critical vulnerabilities reported each year, reflecting both its widespread use and possibly its greater emphasis on reporting and patching vulnerabilities, it's worth noting that Chrome's critical vulnerabilities dropped by 30% in 2023, suggesting improvements. Another explanation for this could be a change in classification or reporting mechanisms, as the number of medium vulnerabilities increased by 15%.

Notably, Chrome reduced its exploited vulnerabilities by 50% in 2023, totaling 5 and bringing it to the same number as Firefox, indicating security improvements. However, its tally of exploited vulnerabilities over three years - 21 - is the highest among the web browsers analyzed, suggesting Chrome may be a more targeted browser for attackers, likely due to its massive user base.

The trends and facts underscore the continued need for aggressive vulnerability management, timely patching, and the importance of security research to uncover and mitigate potential threats across all browsers.

VPN Clients

TABLE 23. VPN CLIENTS 2023 VULNERABILITIES ANALYSIS

Name	All Vulnerabilities 2023	YoY 2023-2022	Critical 2023	YoY 2023-2022	Medium 2023	YoY 2023-2022	Low 2023	YoY 2023-2022	RCE 2023	YoY 2023-2022	Exploited 2023	YoY 2023-2022
VPN Clients	16	33%	10	0%	5	150%	1	N/A	1	0%	0	N/A
Cisco	3	N/A	1	N/A	2	N/A	0	N/A	1	N/A	0	N/A
FortiClient	9	13%	7	17%	1	-50%	1	N/A	0	-100%	0	N/A
OpenVPN	3	-25%	2	-50%	1	N/A	0	N/A	0	N/A	0	N/A
WireGuard	1	N/A	0	N/A	1	N/A	0	N/A	0	N/A	0	N/A

TABLE 24. VPN CLIENTS 2022 VULNERABILITIES ANALYSIS

Name	All Vulnerabilities 2022	YoY 2022-2021	Critical 2022	YoY 2022-2021	Medium 2022	YoY 2022-2021	Low 2022	YoY 2022-2021	RCE 2022	YoY 2022-2021	Exploited 2022	YoY 2022-2021
VPN Clients	12	-63%	10	-55%	2	-80%	0	N/A	1	-91%	0	N/A
Cisco	0	-100%	0	-100%	0	N/A	0	N/A	0	-100%	0	N/A
FortiClient	8	14%	6	50%	2	-33%	0	N/A	1	N/A	0	N/A
OpenVPN	4	-56%	4	-43%	0	N/A	0	N/A	0	N/A	0	N/A
WireGuard	0	-100%	0	N/A	0	N/A	0	N/A	0	N/A	0	N/A

The data reveals that Fortinet is the only VPN client vendor experiencing a consistent rise in total vulnerabilities within its FortiClient software. In 2023, vulnerabilities increased by 13%, following a 14% increase in 2022 - a worrisome trend. Notably, FortiClient holds the highest vulnerability count, totaling 24 from 2021 to 2023. Furthermore, its critical vulnerabilities have seen a rapid surge, rising by 50% in 2022 and by 17% in 2023 - highlighting further cause for concern.

FortiClient is the only VPN client experiencing a consistent rise in total vulnerabilities over years.

OpenVPN's vulnerabilities show a steady decrease over the years, suggesting efforts to improve security. Specifically, vulnerabilities dropped by 56% in 2022 and by 25% in 2023. Data from 2021-2023 reveals a consistent presence of critical vulnerabilities, with 13 out of 16 total. Concurrently, their number decreases each year from 7 in 2021 to 2 in 2023, indicating a positive trend. Interestingly, no RCE vulnerabilities have been reported during this period.

Cisco AnyConnect shows a significant decrease in vulnerability numbers starting in 2021. It is the only VPN client which reported a significant number of RCEs, 12, mainly in 2021. However, none of the VPN client vulnerabilities were exploited, which is positive.

WireGuard has the lowest number of reported vulnerabilities compared to other products analyzed, with only two reported, neither critical nor RCE, nor exploited. This suggests that it is either more secure or less targeted.

The number of vulnerabilities reported not only reflects the security of a certain VPN client but could also indicate its popularity, the attention of its community, and possibly its transparency in reporting vulnerabilities. While WireGuard presents itself as the client with the fewest disclosed vulnerabilities, caution should be exercised in interpreting this as greater security without considering other factors such as market penetration and the extent of third-party security auditing. For Cisco AnyConnect and FortiClient, the higher numbers, especially for critical vulnerabilities, highlight the importance of constant vigilance, rapid patching protocols, and perhaps more in-depth security auditing.

Load Balancers

TABLE 25. LOAD BALANCERS 2023 VULNERABILITIES ANALYSIS

Name	All Vulnerabilities 2023	YoY 2023-2022	Critical 2023	YoY 2023-2022	Medium 2023	YoY 2023-2022	Low 2023	YoY 2023-2022	RCE 2023	YoY 2023-2022	Exploited 2023	YoY 2023-2022
LoadBalancers	14	100%	13	225%	1	-67%	0	N/A	1	N/A	5	N/A
HaProxy	⚠️ 6	500%	⚠️ 5	400%	1	N/A	0	N/A	0	N/A	0	N/A
Citrix	⚠️ 7	N/A	⚠️ 7	N/A	0	N/A	0	N/A	1	N/A	⚠️ 4	N/A
NGINX	1	-83%	1	-67%	0	N/A	0	N/A	0	N/A	1	N/A

TABLE 26. LOAD BALANCERS 2022 VULNERABILITIES ANALYSIS

Name	All Vulnerabilities 2022	YoY 2022-2021	Critical 2022	YoY 2022-2021	Medium 2022	YoY 2022-2021	Low 2022	YoY 2022-2021	RCE 2022	YoY 2022-2021	Exploited 2022	YoY 2022-2021
LoadBalancers	7	-22%	4	-50%	3	200%	0	N/A	0	N/A	0	N/A
HaProxy	1	-75%	1	-67%	0	N/A	0	N/A	0	N/A	0	N/A
Citrix	0	-100%	0	-100%	0	N/A	0	N/A	0	N/A	0	N/A
NGINX	6	100%	3	0%	3	N/A	0	N/A	0	N/A	0	N/A

Despite the relatively low total number of vulnerabilities, load balancers saw a significant number of vulnerabilities exploited in 2023, with CitrixBleed as the most notable one (5 exploited out of 14 total vulnerabilities). The total vulnerabilities for load balancers increased by 100% in 2023, rising from 7 in 2022 to 14 in 2023. Interestingly, HaProxy and Citrix both show that all vulnerabilities discovered in their systems in 2023 were critical, indicating their severity.

Despite having fewer critical vulnerabilities compared to operating systems, load balancers have a record exploitation rate in our research of 17%, which marks a new trend of the increased attractiveness of this group as a target for threat actors, likely due to the critical position of load balancers in network architectures. A single exploit in these systems can provide broad access or disruption capabilities against targeted networks.

Citrix shows 9 vulnerabilities over the three-year period analyzed, with a notable spike in 2023. Citrix experienced a significant security challenge last year, with all of its reported vulnerabilities being both critical and exploited, all due to the devastating vulnerability known as CitrixBleed, which was used in massive cyberattacks on organizations and whose exploit is still in the arsenal of many APTs. Citrix is the only load balancer of the three to have a devastating RCE vulnerability, which is particularly concerning given that RCE vulnerabilities allow attackers to execute arbitrary commands on the affected system. HaProxy and NGINX did not have any RCE vulnerabilities over the three years, indicating either a robust design against such vulnerabilities or effective mitigation strategies. Finally, Citrix's vulnerabilities in 2023 were not only critical but also exploited, making it the most vulnerable load

balancer in terms of actual attacks and breaches of the three in that year.

NGINX shows variability over the years, with a drop to only one vulnerability in 2023, but an increase in 2022. The single vulnerability in 2023 was critical and exploited, indicating that while the number may be low, the impact is significant.

The statistics present an interesting contrast where Citrix had fewer total vulnerabilities than HaProxy over three years, but had one year (2023) where all of its vulnerabilities were rated critical and exploited. This contrast highlights how the severity and exploitation of vulnerabilities can be more telling than their number.

In 2023, Citrix had fewer vulnerabilities than HaProxy, but all were critical and exploited, showing severity matters more than quantity.

The analysis suggests that while load balancers are generally secure with a low number of reported vulnerabilities, the severity and exploitation of these vulnerabilities can vary widely.

Databases

TABLE 27. DATABASES 2023 VULNERABILITIES ANALYSIS

Name	All Vulnerabilities 2023	YoY 2023-2022	Critical 2023	YoY 2023-2022	Medium 2023	YoY 2023-2022	Low 2023	YoY 2023-2022	RCE 2023	YoY 2023-2022	Exploited 2023	YoY 2023-2022
Databases	68	-44%	21	163%	44	-55%	3	-82%	20	1900%	0	-100%
MYSQL	41	-64%	1	-67%	38	-60%	2	-88%	0	N/A	0	-100%
Postgresql	9	50%	3	0%	5	67%	1	N/A	3	N/A	0	N/A
MSSQL	18	800%	17	750%	1	N/A	0	N/A	17	1600%	0	N/A
Oracle DB	10	233%	1	N/A	5	67%	4	N/A	0	N/A	0	N/A

TABLE 28. DATABASES 2022 VULNERABILITIES ANALYSIS

Name	All Vulnerabilities 2022	YoY 2022-2021	Critical 2022	YoY 2022-2021	Medium 2022	YoY 2022-2021	Low 2022	YoY 2022-2021	RCE 2022	YoY 2022-2021	Exploited 2022	YoY 2022-2021
Databases	122	-8%	8	0%	97	-20%	17	750%	1	-50%	2	N/A
MYSQL	114	-8%	3	-25%	94	-20%	17	750%	0	N/A	2	N/A
Postgresql	6	-14%	3	0%	3	-25%	0	N/A	0	-100%	0	N/A
MSSQL	2	100%	2	100%	0	N/A	0	N/A	1	N/A	0	N/A
Oracle DB	3	-57%	0	N/A	3	-50%	0	-100%	0	N/A	0	N/A

MSSQL reports an astonishing 17 critical vulnerabilities out of a total of 18 in 2023, marking a 750% spike in critical vulnerability numbers. All reported critical vulnerabilities were RCEs, raising significant concerns. This pattern is in stark contrast to previous years, requiring immediate attention from database administrators and cybersecurity teams. It indicates not only the discovery of more serious vulnerabilities but also a potential increase in the attractiveness of MSSQL as a target for attackers.

MSSQL reports an astonishing 17 RCE vulnerabilities out of a total of 18 in 2023, indicating increased attractiveness for attackers.

Although MySQL stands out with the highest total number of reported vulnerabilities over the three years (279) compared to other databases, its 64% decrease in total vulnerabilities number in 2023 is promising. MySQL's higher number of vulnerabilities may reflect its popularity and extensive reporting mechanisms. An interesting fact is that while its total number of vulnerabilities is 12 times higher than in MSSQL, its number of critical vulnerabilities is 17 times lower than in MSSQL.

However, MySQL is the only database in this analysis that has reported exploited vulnerabilities, albeit only 2 over the entire period. This suggests that while vulnerabilities are prevalent, the exploitation rate may not be as high, or at least not as widely reported.

PostgreSQL reported a consistent number of 3 critical vulnerabilities each year. Notably, PostgreSQL has a moderate but notable presence of RCE vulnerabilities, with 5 over the period analyzed, which is proportionally significant given its 22 total number of vulnerabilities reported over three years. This indicates that while its vulnerabilities number might not be high, their severity and potential impact are serious.

Oracle DB shows a consistently low to moderate number of vulnerabilities. Variations over the years are minimal, suggesting a steady state of security concerns. Just like MySQL, it reported a low number of critical vulnerabilities compared to its total number of vulnerabilities, indicating a wider distribution of vulnerability severity.

The relative stability of PostgreSQL and Oracle DB in terms of vulnerability numbers underscores a potentially effective security management approach.

This comparison illustrates the dynamic nature of database security, highlighting the importance of proactive vulnerability detection, timely patching, and adapting security measures to evolving threats. It also underscores the critical role of the security community in identifying and reporting vulnerabilities, thereby supporting the collective defense against potential database exploits.

Recommendations

The changing vulnerability landscape highlighted in the research requires organizations to constantly monitor emerging threats and adjust their security strategies to address these evolving risks. Here are the recommendations we derived based on the research:

1. The data shows that operating systems and web browsers have the highest total number of vulnerabilities, including critical and exploited vulnerabilities, which is indicative of their widespread use and complex functionality.
2. Given the high number of critical vulnerabilities in desktop operating systems and mobile operating systems, organizations should prioritize these systems in their patch management programs and allocate resources and time to ensure that these systems are updated in a timely manner. The significant presence of RCE, especially in desktop operating systems, requires robust monitoring and rapid action to mitigate potential threats before they are exploited.
3. The exploited vulnerabilities in web browsers highlight the importance of educating end-users on safe browsing practices, timely patching, and the need to deploy additional security solutions to monitor and control web traffic.
4. Most vulnerabilities require specific actions by employees to be exploited. So, educate employees about the potential risks associated with using corporate applications, especially Microsoft Office, and the importance of following security best practices, such as avoiding suspicious attachments or links, even in seemingly safe documents.
5. While the report does not analyze all available application groups, it offers an actionable example for CIOs and CISOs, illustrating a similar analysis that should be applied to all categories of software used within the organization. This is particularly important for systems exposed to the Internet, as well as those integral to business operations or containing sensitive data. Specifically, such an analysis should cover not only critical software groups like operating systems but also lesser-known software groups (e.g., image editors, password managers) in their vulnerability management framework, especially as the research has recognized that any software can be an attack vector.
6. When choosing third-party software, conduct a comprehensive risk assessment that covers not only the number of vulnerabilities but also their severity and the software vendor's response time to patch those vulnerabilities. While software with fewer vulnerabilities may appear to be more secure, the severity of those vulnerabilities might be critical. Software with fewer exploited vulnerabilities may indicate better security; however, it's important to consider the criticality of the software to the organization's operations. In fact, the extent to which a certain software can be called vulnerable depends more on how the vendor manages its existing vulnerabilities (e.g., timely patching, mitigation strategies) than on the total number of vulnerabilities. Additionally, the functionality of software with low vulnerabilities may be poorer than that of software with higher vulnerabilities and might not meet the organization's needs.

In summary, a CISO should ensure that their organization has robust security measures in place, including regular updates, employee awareness training, and advanced threat detection and response mechanisms. A CISO's role is not only to address current vulnerabilities but also to anticipate potential future vulnerabilities based on trends and improve their organization's security posture to quickly adapt to new threats.

Appendix

TABLE 29. TOTAL VULNERABILITIES 2023

Name	All Vulnerabilities 2023	YoY 2023-2022	Critical 2023	YoY 2023-2022	Medium 2023	YoY 2023-2022	Low 2023	YoY 2023-2022	RCE 2023	YoY 2023-2022	Exploited 2023	YoY 2023-2022
Total	4359	-2%	2254	-15%	2023	22%	82	-41%	540	1%	107	22%

TABLE 30. TOTAL VULNERABILITIES 2022

Name	All Vulnerabilities 2022	YoY 2022-2021	Critical 2022	YoY 2022-2021	Medium 2022	YoY 2022-2021	Low 2022	YoY 2022-2021	RCE 2022	YoY 2022-2021	Exploited 2022	YoY 2022-2021
Total	4449	13%	2658	6%	1653	20%	138	156%	536	3%	88	19%

TABLE 31. TOTAL VULNERABILITIES 2021

Name	All Vulnerabilities 2021	Critical 2021	Medium 2021	Low 2021	RCE 2021	Exploited
Total	3942	2515	1373	54	519	74

TABLE 32. OVERALL VULNERABILITIES

Name	Total Vulnerabilities	Total RCE	Total Exploited	Exploitation Rate, %
Total	12750	1595	269	2

TABLE 33. DESKTOP OS VULNERABILITIES 2021

Name	All Vulnerabilities 2021	Critical 2021	Medium 2021	Low 2021	RCE 2021	Exploited 2021
Desktop Operating Systems	1614	1148	451	15	309	43
MS Windows 10	487	379	107	1	115	15
MS Windows Server 2016	503	390	112	1	126	16
MacOS	462	299	158	5	63	12
Linux	162	80	74	8	5	0

TABLE 34. DESKTOP OS VULNERABILITIES 2023-2021 SUMMARY

Name	Total All Vulnerabilities	Total RCE	Total Exploited	Exploitation Rate, %
Desktop Operating Systems	4885	1096	155	3
MS Windows 10	1497	415	52	3
MS Windows Server 2016	1518	460	52	3
MacOS	1086	195	42	4
Linux	784	26	9	1

TABLE 35. MOBILE OS VULNERABILITIES 2021 ANALYSIS

Name	All Vulnerabilities 2021	Critical 2021	Medium 2021	Low 2021	RCE 2021	Exploited 2021
Mobile Operating Systems	1154	641	477	36	68	14
iOS	380	237	132	11	39	14
Android	656	318	317	21	28	0
HarmonyOs	118	86	28	4	1	0

TABLE 36. MOBILE OS VULNERABILITIES SUMMARY 2021-2023

Name	Total Vulnerabilities	Total RCE	Total Exploited	Exploitation Rate, %
Mobile Operating Systems	4760	224	48	1
iOS	891	154	44	5
Android	3300	69	4	0.12
HarmonyOs	569	1	0	0

TABLE 37. OFFICE APPS 2021 VULNERABILITIES ANALYSIS

Name	All Vulnerabilities 2021	Critical 2021	Medium 2021	Low 2021	RCE 2021	Exploited 2021
Office Apps	115	99	16	0	50	7
Microsoft Office	104	91	13	0	50	7
Libre Office	4	3	1	0	0	0
Open Office	7	5	2	0	0	0

TABLE 38. OFFICE APPS VULNERABILITIES SUMMARY 2021-2023

Name	Total Vulnerabilities	Total RCE	Total Exploited	Exploitation Rate, %
Office Apps	279	110	14	5
Microsoft Office	253	109	14	6
Libre Office	14	1	0	0
Open Office	12	0	0	0

TABLE 39. REMOTE MANAGEMENT SOFTWARE 2021 VULNERABILITY ANALYSIS

Name	All Vulnerabilities 2021	Critical 2021	Medium 2021	Low 2021	RCE 2021	Exploited 2021
Remote Management Software	9	7	2	0	1	0
TeamViewer	2	2	0	0	1	0
DameWare	1	1	0	0	0	0
Splashtop	2	2	0	0	0	0
AnyDesk	3	2	1	0	0	0
RealVNC	1	0	1	0	0	0

TABLE 40. REMOTE MANAGEMENT SOFTWARE VULNERABILITY SUMMARY 2021-2023

Name	Total Vulnerabilities	Total RCE	Total Exploited	Exploitation Rate, %
Remote Management Software	17	3	0	0
TeamViewer	6	3	0	0
DameWare	1	0	0	0
Splashtop	2	0	0	0
AnyDesk	5	0	0	0
RealVNC	3	0	0	0

TABLE 41. DOCUMENT VIEWERS 2021 VULNERABILITY ANALYSIS

Name	All Vulnerabilities 2021	Critical 2021	Medium 2021	Low 2021	RCE 2021	Exploited 2021
Document Viewers	193	132	61	0	64	2
Adobe Reader	92	58	34	0	1	2
Foxit Reader	98	71	27	0	63	0
Nitro PDF	3	3	0	0	0	0

TABLE 42. DOCUMENT VIEWERS VULNERABILITY SUMMARY 2021-2023

Name	Total Vulnerabilities	Total RCE	Total Exploited	Exploitation Rate, %
Document Viewers	418	78	4	1
Adobe Reader	310	14	4	1
Foxit Reader	105	64	0	0
Nitro PDF	3	0	0	0

TABLE 43. PASSWORD MANAGERS 2021 VULNERABILITY ANALYSIS

Name	All Vulnerabilities 2021	Critical 2021	Medium 2021	Low 2021	RCE 2021	Exploited 2021
Password Manager Clients	3	0	3	0	1	0
Keepass	0	0	0	0	0	0
Keepass XC	0	0	0	0	0	0
1Password	3	0	3	0	1	0
Bitwarden	0	0	0	0	0	0
LastPass	0	0	0	0	0	0

TABLE 44. PASSWORD MANAGERS VULNERABILITY SUMMARY 2021-2023

Name	Total Vulnerabilities	Total RCE	Total Exploited	Exploitation Rate, %
Password Manager Clients	12	1	0	0
Keepass	3	0	0	0
Keepass XC	1	0	0	0
1Password	5	1	0	0
Bitwarden	3	0	0	0
LastPass	0	0	0	0

TABLE 45. ANTIVIRUSES 2021 VULNERABILITY ANALYSIS

Name	All Vulnerabilities 2021	Critical 2021	Medium 2021	Low 2021	RCE 2021	Exploited 2021
Antivirus	45	31	14	0	4	1
Avast	7	6	1	0	0	0
Bitdefender	14	10	4	0	3	0
Malwarebytes	1	1	0	0	0	0
Eset	2	0	2	0	0	0
Kaspersky	8	5	3	0	0	0
McAfee	13	9	4	0	1	1

TABLE 46. ANTIVIRUSES VULNERABILITY SUMMARY 2021-2023

Name	Total Vulnerabilities	Total RCE	Total Exploited	Exploitation Rate, %
Antivirus	86	7	1	1
Avast	17	1	0	0
Bitdefender	22	3	0	0
Malwarebytes	8	0	0	0
Eset	10	0	0	0
Kaspersky	11	1	0	0
McAfee	18	2	1	6

TABLE 47. IMAGE EDITORS 2021 VULNERABILITY ANALYSIS

Name	All Vulnerabilities 2021	Critical 2021	Medium 2021	Low 2021	RCE 2021	Exploited 2021
Image Editors	31	27	4	0	2	0
Adobe Photoshop	15	14	1	0	0	0
Gimp	1	1	0	0	0	0
Paint.Net	0	0	0	0	0	0
Adobe Illustrator	15	12	3	0	2	0

TABLE 48. IMAGE EDITORS 2021 VULNERABILITY ANALYSIS

Name	Total Vulnerabilities	Total RCE	Total Exploited	Exploitation Rate, %
Image Editors	130	8	0	0
Adobe Photoshop	58	4	0	0
Gimp	3	0	0	0
Paint.Net	0	0	0	0
Adobe Illustrator	69	4	0	0

TABLE 49. WEB BROWSERS 2021 VULNERABILITY ANALYSIS

Name	All Vulnerabilities 2021	Critical 2021	Medium 2021	Low 2021	RCE 2021	Exploited 2021
Web Browsers	568	366	201	1	6	7
Chrome	353	250	103	0	5	6
Firefox	134	64	69	1	0	0
Edge	81	52	29	0	1	1

TABLE 50. WEB BROWSERS VULNERABILITY SUMMARY 2021-2023

Name	Total Vulnerabilities	Total RCE	Total Exploited	Exploitation Rate, %
Web Browsers	1655	26	39	2
Chrome	1006	10	21	2
Firefox	471	2	11	2
Edge	178	14	7	4

TABLE 51. VPN CLIENTS 2021 VULNERABILITY ANALYSIS

Name	All Vulnerabilities 2021	Critical 2021	Medium 2021	Low 2021	RCE 2021	Exploited 2021
VPN Clients	32	22	10	0	11	0
Clisco Any Connect	15	11	4	0	11	0
FortiClient	7	4	3	0	0	0
OpenVPN	9	7	2	0	0	0
WireGuard	1	0	1	0	0	0

TABLE 52. VPN CLIENTS VULNERABILITY ANALYSIS SUMMARY 2021-2023

Name	Total Vulnerabilities	Total RCE	Total Exploited	Exploitation Rate, %
VPN Clients	60	13	0	0
Clisco Any Connect	18	12	0	0
FortiClient	24	1	0	0
OpenVPN	16	0	0	0
WireGuard	2	0	0	0

TABLE 53. LOAD BALANCERS 2021 VULNERABILITY ANALYSIS

Name	All Vulnerabilities 2021	Critical 2021	Medium 2021	Low 2021	RCE 2021	Exploited 2021
LoadBalancers	9	8	1	0	0	0
HaProxy	4	3	1	0	0	0
Citrix	2	2	0	0	0	0
NGINX	3	3	0	0	0	0

TABLE 54. LOAD BALANCERS VULNERABILITY SUMMARY

Name	Total Vulnerabilities	Total RCE	Total Exploited	Exploitation Rate, %
LoadBalancers	30	1	5	17
HaProxy	11	0	0	0
Citrix	9	1	4	44
NGINX	10	0	1	10

TABLE 55. DATABASES 2021 VULNERABILITY ANALYSIS

Name	All Vulnerabilities 2021	Critical 2021	Medium 2021	Low 2021	RCE 2021	Exploited 2021
Databases	132	8	122	2	2	0
MYSQL	124	4	118	2	0	0
Postgresql	7	3	4	0	2	0
MSSQL	1	1	0	0	0	0
Oracle DB	7	0	6	1	0	0

TABLE 56. DATABASES VULNERABILITY SUMMARY 2021-2023

Name	Total Vulnerabilities	Total RCE	Total Exploited	Exploitation Rate, %
Databases	322	23	2	1
MYSQL	279	0	2	1
Postgresql	22	5	0	0
MSSQL	21	18	0	0
Oracle DB	20	0	0	0

TABLE 57. TOP EXPLOITED SOFTWARE SUMMARY 2021-2023

Category Name	Total Exploitation Rate, %
Citrix	44
NGINX	10
McAfee	6
Microsoft Office	6
iOS	5
Edge	4
MacOS	4
MS Windows 10	3
MS Windows Server 2016	3
Firefox	2

TABLE 58. TOP EXPLOITED SOFTWARE 2022

Category Name	Exploitation Rate 2022, %
Edge	5
iOS	4
MS Windows 10	4
Firefox	4
MS Windows Server 2016	4
MacOS	3
Chrome	3
Linux	2
MYSQL	2
Microsoft Office	2

TABLE 59. TOP EXPLOITED SOFTWARE 2021

Category Name	Exploitation Rate 2021, %
McAfee	8
Microsoft Office	7
iOS	4
MS Windows Server 2016	3
MS Windows 10	3
MacOS	3
Adobe Reader	2
Chrome	2
Edge	1

TABLE 60. EXPLOITATION RATES OF SOFTWARE PER CATEGORY 2021-2023

Software Category	Name	Exploitation Rate 2021	Exploitation Rate 2022	Exploitation Rate 2023
Desktop Operating Systems	MS Windows 10	3.1%	3.8%	3.5%
	MS Windows Server 2016	3.2%	3.5%	3.6%
	MacOS	2.6%	3.3%	6.9%
	Linux	0.0%	1.9%	1.0%
Mobile Operating Systems	iOS	3.7%	4.1%	7.5%
	Android	0.0%	0.1%	0.2%
	HarmonyOs	0.0%	0.0%	0.0%
Office Packets	Microsoft Office	6.7%	1.6%	7.1%
	Libre Office	0.0%	0.0%	0.0%
	Open Office	0.0%	0.0%	0.0%
Remote Management Software	TeamViewer	0.0%	0.0%	0.0%
	DameWare	0.0%	0.0%	0.0%
	Splashtop	0.0%	0.0%	0.0%
	AnyDesk	0.0%	0.0%	0.0%
	RealVNC	0.0%	0.0%	0.0%
Document Viewers	Adobe Reader	2.2%	0.0%	2.2%
	Foxit Reader	0.0%	0.0%	0.0%
	Nitro PDF	0.0%	0.0%	0.0%

Software Category	Name	Exploitation Rate 2021	Exploitation Rate 2022	Exploitation Rate 2023
Password Manager Clients	Keepass	0.0%	0.0%	0.0%
	Keepass XC	0.0%	0.0%	0.0%
	1Password	0.0%	0.0%	0.0%
	Bitwarden	0.0%	0.0%	0.0%
	Lastpass	0.0%	0.0%	0.0%
Antiviruses	Avast	0.0%	0.0%	0.0%
	Bitdefender	0.0%	0.0%	0.0%
	Malwarebytes	0.0%	0.0%	0.0%
	Eset	0.0%	0.0%	0.0%
	Kaspersky	0.0%	0.0%	0.0%
	McAfee	7.7%	0.0%	0.0%
Image Editors	Adobe Photoshop	0.0%	0.0%	0.0%
	Gimp	0.0%	0.0%	0.0%
	Paint.Net	0.0%	0.0%	0.0%
	Adobe Illustrator	0.0%	0.0%	0.0%
Web Browsers	Chrome	1.7%	2.8%	1.7%
	Firefox	0.0%	3.8%	2.8%
	Edge	1.2%	5.4%	6.7%
VPN Clients	Cisco Any Connect	0.0%	0.0%	0.0%
	FortiClient	0.0%	0.0%	0.0%
	OpenVPN	0.0%	0.0%	0.0%
	WireGuard	0.0%	0.0%	0.0%

Software Category	Name	Exploitation Rate 2021	Exploitation Rate 2022	Exploitation Rate 2023
Load Balancers	HaProxy	0.0%	0.0%	0.0%
	Citrix	0.0%	0.0%	57.1%
	NGINX	0.0%	0.0%	100.0%
Databases	MYSQL	0.0%	1.8%	0.0%
	Postgresql	0.0%	0.0%	0.0%
	MSSQL	0.0%	0.0%	0.0%
	Oracle DB	0.0%	0.0%	0.0%

About Action1 Research

The report is brought to you by Action1 Research, which conducts industry surveys among cybersecurity practitioners worldwide to discover trends in cybersecurity. For more information, please visit:

www.action1.com/resources/research/

About Action1 Corporation

Action1 reinvents patch management with an infinitely scalable and highly secure platform configurable in 5 minutes that just works. With integrated real-time vulnerability assessment and automated remediation for third-party software and OS, peer-to-peer patch distribution, and IT ecosystem integrations, it ensures continuous patch compliance and reduces ransomware and security risks – all while lowering costs. Action1 is certified for SOC 2/ISO 27001 and is trusted by thousands of enterprises managing millions of endpoints globally.

Action1 was founded by cybersecurity veterans Alex Vovk and Mike Walters, who previously founded Netwrix, which was acquired by TA Associates. Learn more at: www.action1.com.