Action1

Patching That Just Works

SOFTWARE VULNERABILITY RATINGS REPORT 2025

INTRODUCTION

As organizations around the world continue to digitally expand and rely more heavily on enterprise software, managing software vulnerabilities has become a critical cornerstone of cybersecurity strategies. This ***2025 Software Vulnerability Ratings Report*** provides a comprehensive analysis of vulnerability trends across commonly used enterprise software categories, offering actionable insights for IT and cybersecurity leaders. Similar to previous annual analyses, this document is designed to help CISOs, CIOs, security analysts, and IT operations staff make informed cybersecurity risk assessment, vendor selection, and strategic planning decisions.

The report is based on data from 2021 to 2024. This year's analysis focuses on vulnerability trends in calendar year 2024, examining key indicators such as the total number of vulnerabilities discovered, the rate of exploitation, and the prevalence of critical Remote Code Execution (RCE) vulnerabilities. RCE vulnerabilities continue to be a primary concern due to their severe impact, allowing attackers to remotely execute malicious code, often leading to system compromise and data breaches.

Armed with these insights, cybersecurity leaders and enterprise stakeholders are better positioned to identify critical trends, address software security gaps, and improve their risk mitigation strategies. In addition, organizations that leverage the contents of this report gain an advantage when evaluating software vendors based on their past security performance—enabling strategic partnerships with vendors committed to proactive vulnerability management.

As a result, the ***2025 Software Vulnerability Ratings Report*** serves as a critical tool for assessing cybersecurity risks, efficiently allocating resources, guiding vulnerability management programs, and ultimately protecting critical business systems and sensitive corporate data from an ever-evolving threat landscape.

Table of Contents

EXECUTIVE SUMMARY

The year 2024 saw profound and pivotal developments in the software cybersecurity landscape. Based on an in-depth analysis of vulnerability data aggregated from the *NVD* and *CVEdetails.com*, this report highlights significant shifts across multiple software categories compared to previous years. The following are the five most influential vulnerability trends uncovered in 2024, highlighting key insights derived directly from the vulnerability data analyzed:

Trend 1

Surge in Discovered and Exploited Vulnerabilities

In 2024, the total number of vulnerabilities discovered increased significantly by ***61%***, reaching 6,761 compared to 4,202 in 2023. ***Linux*** saw an unprecedented increase of ***967%***, the largest of any category, with 3,329 vulnerabilities discovered—substantially contributing to the overall rise across all software categories. Similarly, ***macOS*** experienced a significant ***95%*** increase compared to the previous year. Database vulnerabilities also rose sharply by ***213%***, with ***MSSQL*** alone showing a particularly alarming ***567%*** increase in identified vulnerabilities. With the total number of vulnerabilities in the database category rising from 68 in 2023 to 213 in 2024, databases became a major contributor to the overall increase.

More critically, the number of exploited vulnerabilities increased dramatically by ***96%***, from 101 in 2023 to 198 in 2024. Web browsers—particularly ***Google's Chrome*** (***+1840%***, from 5 to 97 exploited vulnerabilities) and ***Microsoft Office*** (***+433%***, from 6 to 32)—are key targets driving this trend. This significant increase demonstrates escalating threat actor activity and underscores the urgent need for organizations to strengthen their vulnerability management and incident response capabilities.

The disparity between the number of vulnerabilities and actual exploitation suggests that cybersecurity practices should focus more on the likelihood of exploitation rather than the mere existence of vulnerabilities. Increases in exploitation can occur even when total vulnerabilities decrease, indicating that attackers may be focusing on fewer but more impactful vulnerabilities.

Trend 2

Sharp increase in critical vulnerabilities

Analysis of the data reveals a significant ***37.1%*** increase in critical vulnerabilities—from 2,137 vulnerabilities in 2023 to 2,930 in 2024. Operating systems—especially ***Linux*** (***+499%***, from 142 to 851 critical vulnerabilities)—and databases—especially ***MSSQL*** (***+606%***, from 17 to 120)—were major contributors to this rise. ***Google Chrome*** saw a notable ***13%*** increase in the number of critical vulnerabilities discovered.

The increase in severity can be attributed to the growing complexity of modern software, as well as intensified efforts by attackers to exploit higher-severity vulnerabilities. IT security teams must prioritize resources and processes to quickly address these critical vulnerabilities in order to avoid serious operational and security consequences.

Trend 3

Dramatic escalation of Linux and macOS vulnerabilities

In 2024, ***Linux*** and ***macOS*** stand out among operating systems with extraordinary increases in vulnerabilities. ***Linux*** vulnerabilities jumped an unprecedented ***967%***, reaching 3,329 identified cases, while ***macOS*** vulnerabilities jumped ***95%***, totaling 508 in 2024. This significant increase for both operating systems signals a growing attacker focus on UNIX-based ecosystems and previously perceived "safer" platforms.

Even more concerning is the sharp increase in critical vulnerabilities, which jumped ***499%***, from 142 in 2023 to 851 in 2024. Critical vulnerabilities on ***Macs*** in particular increased significantly—by ***92%***, from 113 in 2023 to 217 in 2024.

However, one positive trend emerged: a decrease in RCE vulnerabilities for both ***Linux (-85%)*** and ***macOS (-44%)***. Organizations using these operating systems need to re-evaluate and strengthen their defensive strategies and patch management practices.

Trend 4

Escalation of Critical Database Vulnerabilities

Database software showed a remarkable pattern of vulnerability growth, with total vulnerabilities increasing by an alarming ***213%***. Critical vulnerabilities in database solutions increased dramatically, escalating by ***505%*** in 2024. The largest contributors to this trend are ***MSSQL (+606%)*** and ***MySQL (+100%)***.

This troubling trend highlights database platforms as emerging high-value targets for threat actors hunting for sensitive data and underscores the need for diligent, vendor-specific vulnerability management, continuous monitoring, and secure database configuration practices to protect sensitive corporate data.

Trend 5

Increased risk of exploited vulnerabilities in web browsers and office applications

Among widely used applications, web browsers saw a ***657%*** increase in exploited vulnerabilities, along with a ***107%*** rise in RCE vulnerabilities, particularly in the popular ***Google Chrome*** browser, which recorded an alarming ***97*** exploited vulnerabilities—more than any other software product analyzed.

Microsoft Office applications experienced a dramatic ***433%*** increase in exploited vulnerabilities, despite an overall vulnerability decrease (***-54%***), suggesting that attackers are focusing on fewer, previously undiscovered or unpatched vulnerabilities.

As a result, organizations must prioritize the rapid deployment of secure patches and strengthen endpoint defenses in addition to employee-focused security awareness training.

METHODOLOGY

In preparing this report, our analytical methodology remains aligned with *last year's* practice. Data was primarily sourced and aggregated from the *National Vulnerability Database (NVD)* and *CVEdetails.com*, which provide independent, reliable resources for identifying and categorizing vulnerabilities.

Key metrics and criteria presented in this report include:

- ***Exploitation Rate:*** Defined as the percentage of vulnerabilities actively exploited in the wild compared to the total number of vulnerabilities discovered.
- ***Remote Code Execution (RCE) Vulnerabilities:*** Individually highlighted due to their elevated severity and immediate threat to enterprise systems.
- ***Vulnerability Severity Ratings:*** Classified as Critical (CVSS > 7.0), Medium (4.0 ≤ CVSS ≤ 7.0), and Low (CVSS < 4.0) according to the industry-standard CVSS rating system.

Enterprise software categories were defined based on three criteria: popularity, criticality in use by organizations, and the total number of vulnerabilities found. Some categories—such as text editors, 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 exploitation rate formula* is as follows:

$$\frac{\textit{Number of exploited vulnerabilities}}{\textit{Total number of vulnerabilities}} \times 100$$

This metric is valuable because it indicates software's susceptibility to exploitation, highlighting the proactiveness of developers in preventing vulnerabilities rather than merely addressing them after they have been exploited by hackers.

For example, if the metric is high—indicating that most known vulnerabilities were exploited despite a low total number—it can suggest a lack of an efficient vulnerability management process in the vendor's organization. Conversely, if the metric is low—even with a high number of exploited vulnerabilities but a significantly larger total number—it may indicate a functioning vulnerability management process. This could also mean 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 total number, that may signal a robust patch management process in the vendor's organization.

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.

DISCLAIMER:

- The formula only considers the number of exploited vulnerabilities in relation to the total number of known vulnerabilities. It doesn't consider 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 not considered within the formula.

ENTERPRISE SOFTWARE CATEGORIES

Desktop Operating Systems	*Mobile Operating Systems*	*Office Applications*
MS Windows 10	iOS	Microsoft Office
MS Windows Server 2016	Android	LibreOffice
macOS	HarmonyOS	OpenOffice
Linux		

Web Browsers	*Databases*	*Remote Management Apps*
Google Chrome	MySQL	TeamViewer
Firefox	PostgreSQL	DameWare
Microsoft Edge	MSSQL	Splashtop
	Oracle Database	AnyDesk
		RealVNC

PDF Readers	*Password Managers*	*Antivirus Software*
Adobe Reader	KeePass	Avast
Foxit Reader	KeePassXC	Bitdefender
Nitro PDF	1Password	Malwarebytes
	Bitwarden	ESET
	LastPass	Kaspersky
		McAfee

VPN Clients	*Archiving Software*	*Proxy Servers*
Cisco AnyConnect	7-Zip	HAProxy
FortiClient	WinRAR	Citrix
OpenVPN	PowerArchiver	NGINX
WireGuard		

EXPLOITATION RATES

Top 10 Software by Exploitation Rate

Rank	Software	Exploitation Rate 2024	Exploitation Rate 2023	YoY change (%)
1	***Citrix***	28.6%	44.4%	-36%
2	***7-Zip***	25.0%	0.0%	**New!**
3	***WinRAR***	20.0%	50.0%	-60%
4	***Microsoft Office***	15.8%	5.5%	+185%
5	***AnyDesk***	14.3%	0.0%	**New!**
6	***Chrome***	9.3%	2.1%	+347%
7	***TeamViewer***	7.7%	0.0%	**New!**
8	***NGINX***	5.6%	10.0%	-44%
9	***McAfee***	5.0%	5.6%	-10%
10	***Microsoft Edge***	4.6%	3.9%	+17%

Key Analytical Insights

Significant Threat Activity Targeting Archiving Software

Archiving tools **7-Zip** and **WinRAR** were among the most exploited software products in 2024, with exploitation rates of 25% and 20%, respectively. While WinRAR's exploitation rate dropped significantly year-over-year, both tools remained highly attractive to threat actors.

Significant Decline—But Continued High Risk—for Load Balancing Software

Citrix remains highly exploited (28.6%) despite a significant drop (-36%) from last year (44.4%). **NGINX** also saw a 44% decrease but continues to rank in the Top 10.

Remote Management Software Becomes a Key Target

AnyDesk (14.3%) and **TeamViewer** (7.7%) appeared in the Exploitation Rate Top 10 for the first time in 2024, having recorded no exploits in 2023. This trend reflects the growing appeal of remote management tools as high-priority targets for attackers.

Microsoft Office at Increasing Risk

Microsoft Office saw a striking 185% increase in its exploitation rate, rising from 5.5% in 2023 to 15.8% in 2024. This surge indicates growing attacker interest and heightened risk associated with widely used office productivity software.

Browsers Under Increased Attack

Chrome saw its exploitation rate surge by an alarming 347%, from 2.1% to 9.3%, underscoring browser vulnerabilities as a fertile attack vector. **Microsoft Edge** also recorded a notable 17% increase. These findings confirm that Chromium-based browsers are now primary targets for attackers due to their widespread use.

The detailed 2024 data clearly shows that threat actors have increasingly targeted archiving software, office productivity tools, browsers, and remote management solutions—all essential components of modern enterprise environments.

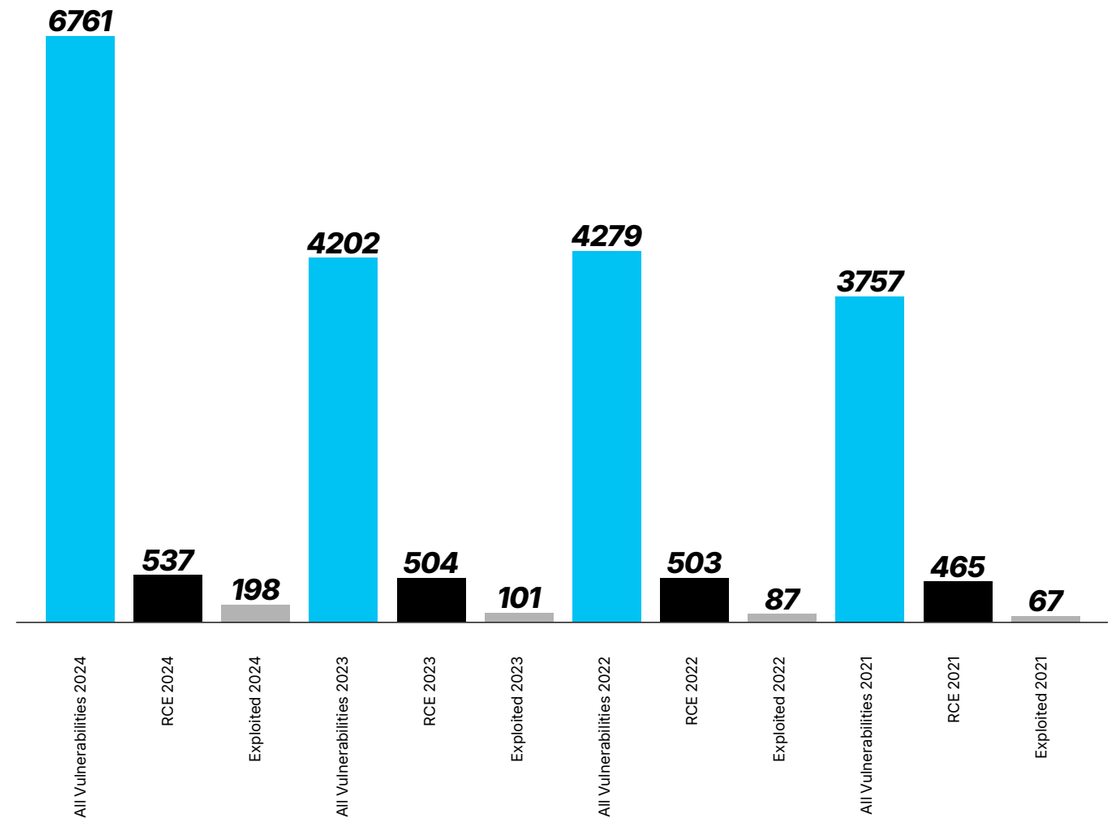
VULNERABILITY ANALYSIS AND TRENDS

Our analysis of software vulnerabilities in 2024 confirms the ongoing rise in software vulnerability disclosures across various software categories. Specifically, 2024 saw notable increases in the total number of vulnerabilities, severity levels (Critical and RCE), and the volume of actively exploited vulnerabilities.

The data underscores a clear upward trend compared to previous years, reflecting a growing intensity of cyber threats. RCE vulnerabilities remain especially concerning, as they allow attackers to execute unauthorized commands remotely—often leading to severe compromise.

Below is a summary table showing the total vulnerabilities, RCE vulnerabilities, and actively exploited vulnerabilities from 2021 to 2024.

Vulnerability Statistics	2024	2023	2022	2021
All Vulnerabilities	***6,761***	***4,202***	***4,279***	***3,757***
RCE Vulnerabilities	***537***	***504***	***503***	***465***
Exploited Vulnerabilities	***198***	***101***	***87***	***67***



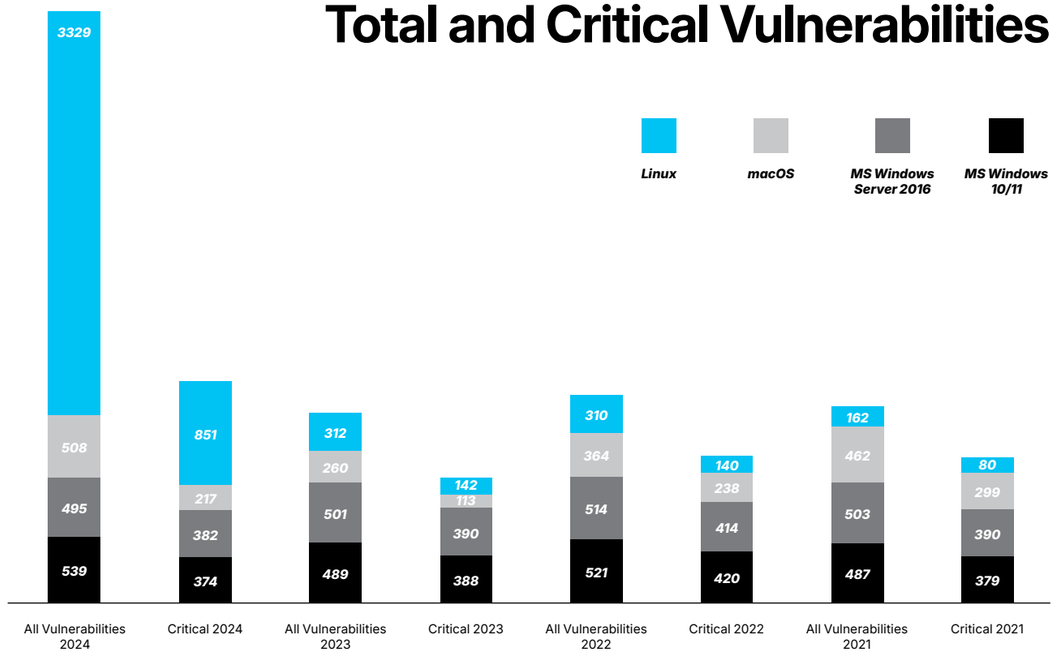
Key Observations

- The ***total number of vulnerabilities*** discovered in 2024 rose by ***61%***, from 4,202 in 2023 to 6,761, marking an accelerating pace of vulnerability emergence. One possible contributing factor is that vendors may be reporting more bugs as CVEs, potentially influenced by less stringent attribution criteria.
- ***RCE vulnerabilities*** increased modestly by ***7%***, from 504 in 2023 to 537 in 2024. Despite the limited growth, RCE remains among the most dangerous vulnerability types due to the high-impact nature of successful exploitation.
- The number of ***actively exploited vulnerabilities*** nearly doubled, rising by ***96%*** from 101 in 2023 to 198 in 2024. This sharp rise indicates that attackers are increasingly prioritizing exploitation of known vulnerabilities as entry points into enterprise systems.
- The consistent year-over-year rise, particularly in critical and exploited vulnerabilities, reinforces the escalating cybersecurity risks facing organizations. To mitigate these risks, enterprises must adopt robust patching processes, enhance threat detection capabilities, conduct thorough vendor and supply chain risk assessments, and continuously improve their security policies and practices.

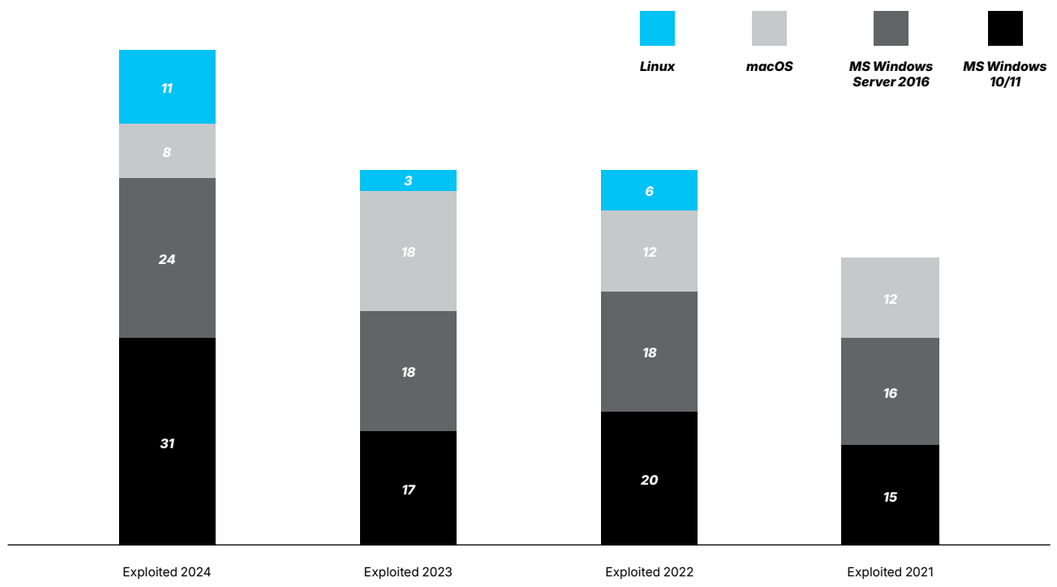
DESKTOP OPERATING SYSTEM

Name	AllVulnerabilities2024	Critical2024	Exploited2024	AllVulnerabilities2023	Critical2023	Exploited2023	AllVulnerabilities2022	Critical2022	Exploited2022	AllVulnerabilities2021	Critical2021	Exploited2021
MS Windows 10/11	539	374	31	489	388	17	521	420	20	487	379	15
MS Windows Server 2016	495	382	24	501	390	18	514	414	18	503	390	16
MacOS	508 +95%	217 +92%	8	260	113	18	364	238	12	462	299	12
Linux	3329 +967%	851 +499%	11 +267%	312	142	3	310	140	6	162	80	0

Total and Critical Vulnerabilities



Exploited Vulnerabilities



Overview

Overall Vulnerability Trends

Linux experienced a dramatic surge in reported vulnerabilities in 2024, with a ***967%*** increase—rising from 312 in 2023 to 3,329. ***MacOS*** followed with a significant ***95%*** increase, reaching 508 vulnerabilities, up from 260 in 2023. In comparison, ***MS Windows 10/11*** saw a moderate ***10%*** rise to 539 vulnerabilities, while ***MS Windows Server 2016*** remained stable, with a slight decrease ***(-1%)*** to 495 vulnerabilities.

Linux Vulnerabilities Spike

The explosion of Linux vulnerabilities is striking. Long regarded as one of the most secure operating systems—thanks to its open-source foundation and collaborative security oversight—Linux is now seeing an unprecedented surge in reported flaws. This raises important questions about current vulnerability assessment, disclosure, and reporting practices across Linux distributions. It may also indicate increased research and attacker focus on Linux environments as the platform becomes more central to enterprise and cloud infrastructure functions.

There is another explanation. In 2024, the Linux kernel was accredited as a CVE Numbering Authority (CNA) by the CVE Program. This designation allows the kernel team to assign CVE identifiers to vulnerabilities they discover and fix. As a result, vulnerability documentation has become more detailed and frequent, contributing to the increased number of CVEs reported. This shift has improved transparency in the disclosure process and enabled more structured kernel security management.

Although the number of reported CVEs has risen, this does not necessarily point to growing system insecurity. On the contrary, it may reflect enhanced documentation and visibility of resolved issues. With more accessible CVE management, even minor bugs are now being classified and reported.

Either way, the sheer increase in Linux vulnerabilities (967%) and critical vulnerabilities (499%) is unexpected and should prompt immediate discussion within the security community about the long-term security posture and vulnerability management practices in the open-source Linux ecosystem.

Critical Vulnerabilities

Linux also stands out in terms of critical vulnerabilities, with a dramatic increase (***499%***, from 142 in 2023 to 851 in 2024). ***MacOS*** also experienced a notable rise (***92%***, from 113 to 217). Conversely, ***Microsoft Windows 10/11*** and ***Windows Server 2016*** demonstrated commendable stability, with ***Windows 10/11*** even showing a slight decrease ***(-4%)*** in critical vulnerabilities (374 total in 2024).

Notably, the number of critical vulnerabilities reported in 2024 alone exceeds the total number of all vulnerabilities reported in 2023.

Medium-Severity Vulnerabilities

In terms of medium-severity issues, ***Linux*** vulnerabilities showed another significant increase (***1171%***) in 2024, reaching 2,110 vulnerabilities. ***MacOS*** medium-severity vulnerabilities also increased sharply (***101%***) to 253. Interestingly, ***Windows 10/11*** experienced a notable jump (***63%***) to a total of 165 medium-severity flaws, highlighting the potential growing complexity or breadth of attack vectors within Windows client environments.

RCE Vulnerabilities

Significantly, ***Windows*** operating systems reported a high number of RCE vulnerabilities. Specifically, ***Windows 10/11*** logged 148 RCEs in 2024, reflecting a slight decrease of ***5%***, while ***Windows Server 2016*** also maintained high RCE figures, reporting 160 in 2024—a year-over-year drop of ***10%***. ***MacOS*** saw a notable ***44%*** decrease, and ***Linux*** maintained minimal RCE activity, reporting only 2 RCE occurrences in 2024, an ***85%*** decline.

The consistently high volume of RCEs in ***Windows*** systems underscores the continued appeal of remotely exploitable flaws in this platform, which remains a primary entry point for attackers targeting enterprise environments. However, the year-over-year reduction in RCEs is a positive development.

Exploited Vulnerabilities

Exploited vulnerabilities are particularly critical because they indicate ongoing, real-world attacker activity. ***Windows 10/11*** exhibited a significant ***82%*** increase in exploited vulnerabilities, rising to 31 cases, underscoring growing interest from targeted attackers. ***Windows Server 2016*** also showed increased targeting, with a ***33%*** rise to 24 cases. ***Linux*** experienced a substantial relative increase of ***267%***, though the absolute number remained low at just 11 incidents. ***MacOS***, meanwhile, saw a ***56%*** decrease, falling to 8 exploited vulnerabilities.

The significant rise in exploited vulnerabilities on ***Windows*** platforms highlights the growing traction attackers are gaining against these widely adopted systems in real-world attacks. In contrast, despite the surge in overall Linux vulnerabilities, active exploitation remains comparatively limited.

Exploitation Rates

The exploitation rate provides insight into the relationship between discovered vulnerabilities and those that are actively exploited. ***Windows*** client and server operating systems showed stable exploitation rates (***4.1%*** and ***3.8%*** respectively, slightly increasing from previous years). However, ***Linux*** had an extremely low exploitation rate (***0.5%***), significantly lower than ***Windows*** or ***macOS***. Interestingly, ***macOS*** had a decreasing exploitation rate (***3.1%*** in 2024, a 19% decline from 2023). The increase in vulnerabilities (95%) and criticality (92%) of ***macOS***, along with a decreasing exploitation rate (-19%), could indicate more proactive research and disclosure, better vendor response, or a shift in attacker preference to other platforms.

The low exploitation rate for ***Linux*** indicates that although vulnerabilities have increased, attackers have found it difficult to effectively exploit ***Linux*** in practice. ***Windows*** and ***macOS*** continue to appear as preferred practical targets, suggesting that these vulnerabilities have a higher likelihood of real-world exploitation—and thus require prioritized security attention.

Despite traditionally perceived Windows-specific targeting, ***Windows*** showed relatively stable and consistent vulnerability reporting, suggesting a more mature and structured vulnerability management approach across the Microsoft ecosystem.

Key Takeaways

- The rise in ***Linux*** vulnerabilities calls for an urgent re-evaluation of patching and assessment processes.
- ***macOS*** needs stronger security oversight amid growing vulnerability volume and severity.
- ***Windows*** remains a key target; timely patching and RCE monitoring are still critical.

MOBILE OPERATING SYSTEM

Name	AllVulnerabilities2024	Critical2024	Exploited2024	AllVulnerabilities2023	Critical2023	Exploited2023	AllVulnerabilities2022	Critical2022	Exploited2022	AllVulnerabilities2021	Critical2021	Exploited2021
IOS	***317***	***126***	***5***	***268***	***121***	***20***	***243***	***155***	***10***	***380***	***237***	***14***
Android	***501***	***299***	***8*** +167%	***1421***	***401***	***3***	***1223***	***494***	***1***	***656***	***318***	***0***
HarmonyOs	***189***	***119***	***0***	***194***	***163***	***0***	***257***	***213***	***0***	***118***	***86***	***0***

Overview

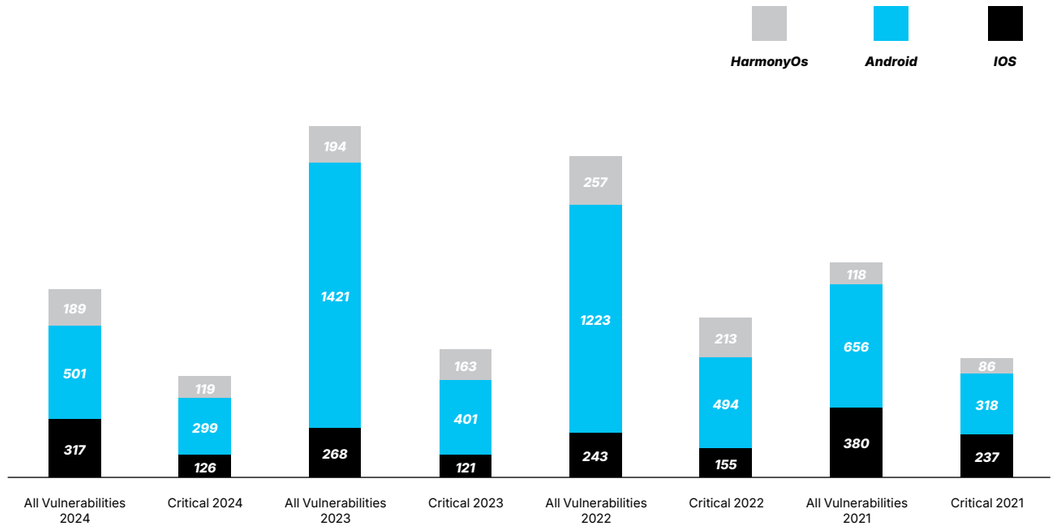
Our data shows that the number of vulnerabilities across mobile operating systems does not follow a consistent upward or downward trend. From 2021 to 2023, there was a steady increase in total vulnerabilities. However, in 2024, we observed a ***47%*** decrease, reflecting the dynamic nature of the mobile threat landscape. This drop is largely due to Android's sharp decline in reported vulnerabilities.

Despite previous increases, ***Android*** experienced a notable ***65%*** decrease in total vulnerabilities in 2024. However, the number of exploited vulnerabilities rose significantly—by ***167%***, driving a ***160%*** increase in ***Android's*** exploitation rate. This highlights a critical insight: fewer reported vulnerabilities do not necessarily mean lower risk. The data suggests that attackers may be becoming more efficient at exploiting existing flaws, a counterintuitive yet important trend.

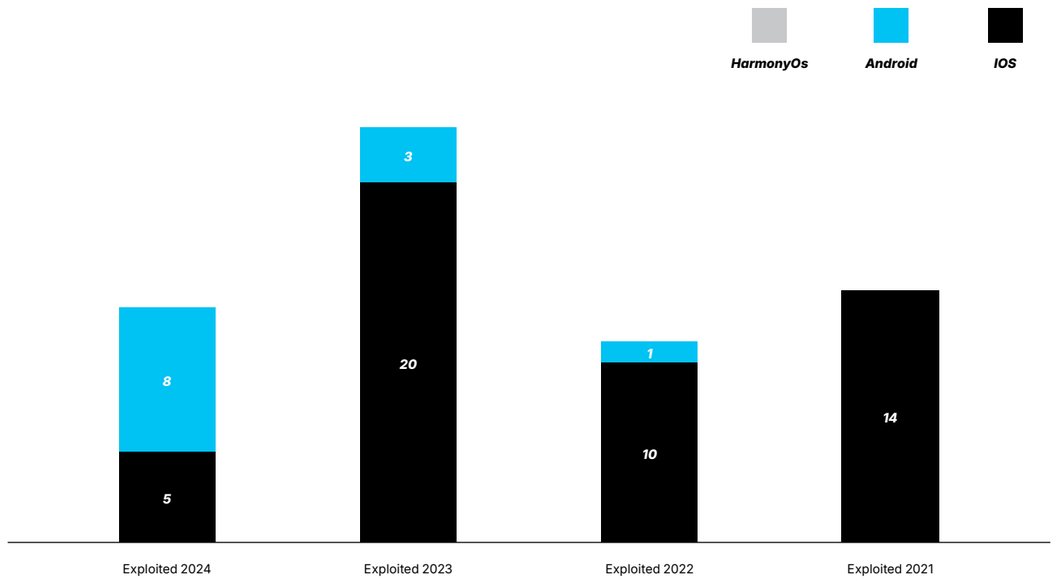
HarmonyOS stands out for its stability. Although it saw a significant increase in critical vulnerabilities in 2022, those numbers stabilized and slightly decreased by 2024. Notably, ***HarmonyOS*** has consistently reported ***no exploited vulnerabilities***, which could be a result of strong security measures or lower adoption rates, making it a less attractive target for attackers.

iOS experienced a moderate ***18%*** increase in total vulnerabilities in 2024. However, the number of exploited vulnerabilities dropped significantly—by ***75%***. This may indicate that Apple has improved its vulnerability handling, and possibly that attackers have shifted their focus away from iOS devices.

Total and Critical Vulnerabilities



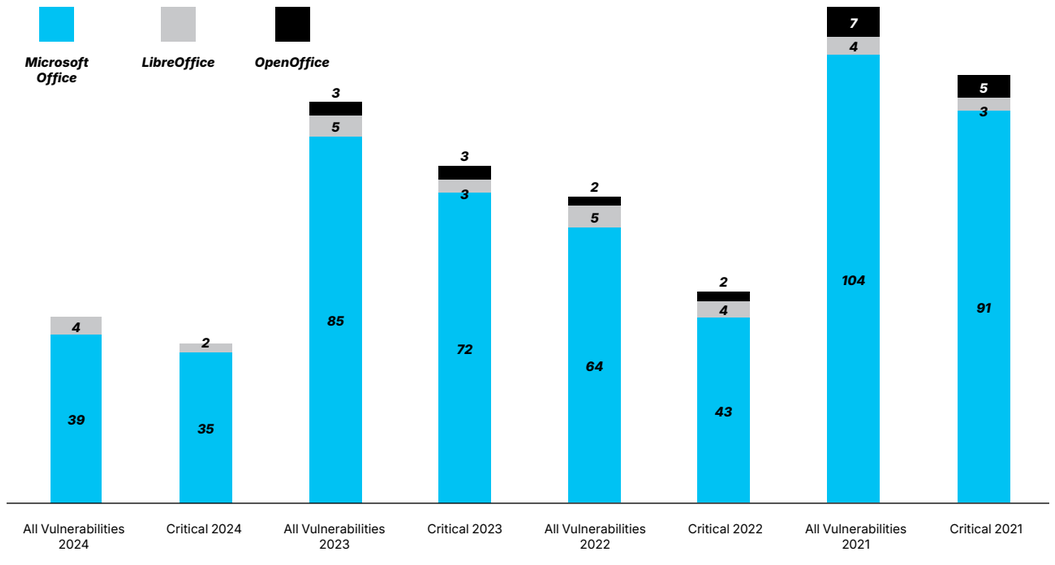
Exploited Vulnerabilities



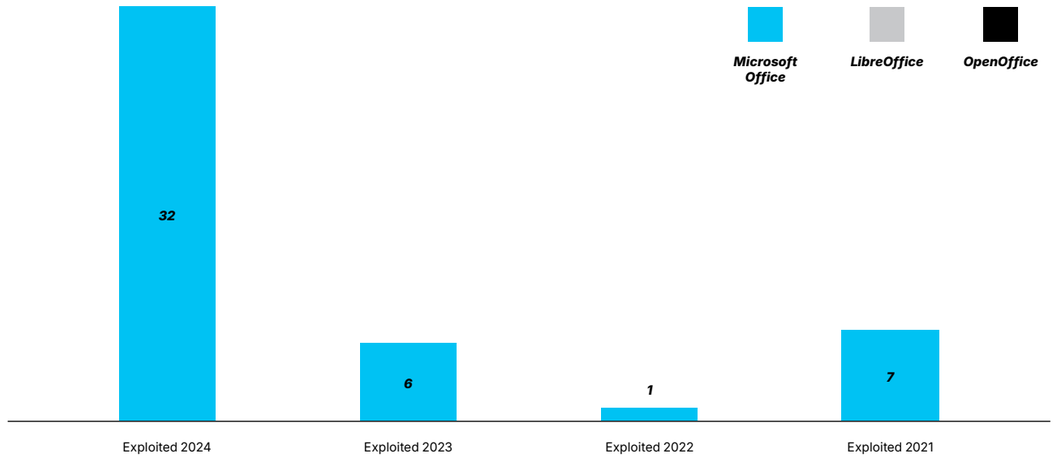
OFFICE APPLICATIONS

Name	AllVulnerabilities2024	Critical2024	Exploited2024	AllVulnerabilities2023	Critical2023	Exploited2023	AllVulnerabilities2022	Critical2022	Exploited2022	AllVulnerabilities2021	Critical2021	Exploited2021
Microsoft Office	***39***	***35***	***32*** ***+433%***	***85***	***72***	***6***	***64***	***43***	***1***	***104***	***91***	***7***
LibreOffice	***4***	***2***	***0***	***5***	***3***	***0***	***5***	***4***	***0***	***4***	***3***	***0***
OpenOffice	***0*** ***-100%***	***0*** ***-100%***	***0***	***3***	***3***	***0***	***2***	***2***	***0***	***7***	***5***	***0***

Total and Critical Vulnerabilities



Exploited Vulnerabilities



Overview

Vulnerability Trends Across Office Suites

The vulnerability landscape for ***Microsoft Office*** has fluctuated over the past four years. After a significant 38% decrease in total vulnerabilities from 2021 to 2022, Microsoft Office experienced a 33% increase in 2023, followed by another sharp ***54%*** drop in 2024. If this cyclical trend continues, a notable increase in total vulnerabilities may occur in 2025. Critical vulnerabilities followed a similar pattern—dropping by 53% in 2022, rising by 67% in 2023, and then falling again by ***51%*** in 2024.

LibreOffice maintained a ***consistently low*** number of vulnerabilities throughout the same period, with total vulnerability counts fluctuating only slightly between 4 and 5. Critical vulnerabilities showed a similar trend with minor increases and decreases.

OpenOffice, on the other hand, experienced a sharp decline in total vulnerabilities—from 7 in 2021 to ***zero*** in 2024. Critical vulnerabilities also dropped to zero. This decline is likely due to stagnation in development; ***OpenOffice***'s last major release (version 4.0) dates back to 2013, with a minor 4.1 release in 2014. The upcoming 4.2 version has no scheduled release date and remains in developer preview as of early 2019. While ***OpenOffice*** is not entirely obsolete, its long-standing security patch delays and inactive development present a significant risk. In contrast, the ***LibreOffice*** community is more responsive in addressing known issues.

Exploitation Trends

Despite an overall drop in total vulnerabilities in 2024, ***Microsoft Office*** saw a dramatic spike in exploited vulnerabilities—from just 6 in 2023 to 32 in 2024, representing a ***433%*** increase. Most of these were RCE vulnerabilities, which pose a severe risk due to common attack vectors such as phishing emails with malicious Office attachments. The exploitation rate for ***Microsoft Office*** rose sharply, from 5.5% in 2023 to 15.8% in 2024—a ***185%*** increase—further underscoring its continued appeal to threat actors.

In contrast, both ***LibreOffice*** and ***OpenOffice*** consistently reported ***no exploited vulnerabilities*** during the analyzed period. While this could indicate a lack of attacker interest, it may also reflect underreporting or reduced visibility due to their smaller user bases. Organizations should be cautious not to dismiss potential risks in these platforms, especially if threat actors begin shifting focus.

WEB BROWSERS

Name	AllVulnerabilities2024	Critical2024	Exploited2024	AllVulnerabilities2023	Critical2023	Exploited2023	AllVulnerabilities2022	Critical2022	Exploited2022	AllVulnerabilities2021	Critical2021	Exploited2021
Chrome	***259***	***204***	***97*** ***+1840%***	***296***	***180***	***5***	***357***	***257***	***10***	***353***	***250***	***6***
Firefox	***187***	***105***	***5***	***180***	***87***	***5***	***157***	***82***	***6***	***134***	***64***	***0***
Edge	***62***	***21***	***4***	***60***	***27***	***4***	***37***	***25***	***2***	***81***	***52***	***1***

Overview

Chrome: Fewer Vulnerabilities, More Exploits

After a slight increase in total vulnerabilities in 2022, ***Google Chrome*** saw declines in both 2023 (-17%) and 2024 (***-13%***). Critical vulnerabilities dropped significantly in 2023 (-30%) but rose again in 2024 (***+13%***). Notably, remote code execution (RCE) vulnerabilities jumped from 5 or fewer in previous years to ***15*** in 2024. Even more striking is the surge in exploited vulnerabilities—rising dramatically to 97 in 2024 (***+1840%***). This spike is unexpected, especially given the overall decline in total vulnerabilities. It may signal increased attacker focus on ***Chrome***, likely driven by its vast user base. The spike in exploited vulnerabilities suggests a growing need for continuous patch management and may prompt organizations to reassess the security risks associated with using Chrome.

Firefox: Rising Severity, Stable Exploits

Mozilla Firefox experienced a steady increase in total vulnerabilities from 2021 to 2023, followed by a modest ***4%*** rise in 2024. Critical vulnerabilities grew steadily, reaching 105 in 2024 (***+21%*** from the previous year). RCE vulnerabilities remained minimal, peaking at 2 in 2023 and dropping to ***1*** in 2024. The number of exploited vulnerabilities remained stable at 5 in both 2023 and 2024, despite rising totals and criticality. This may reflect effective mitigation efforts or reduced interest from attackers.

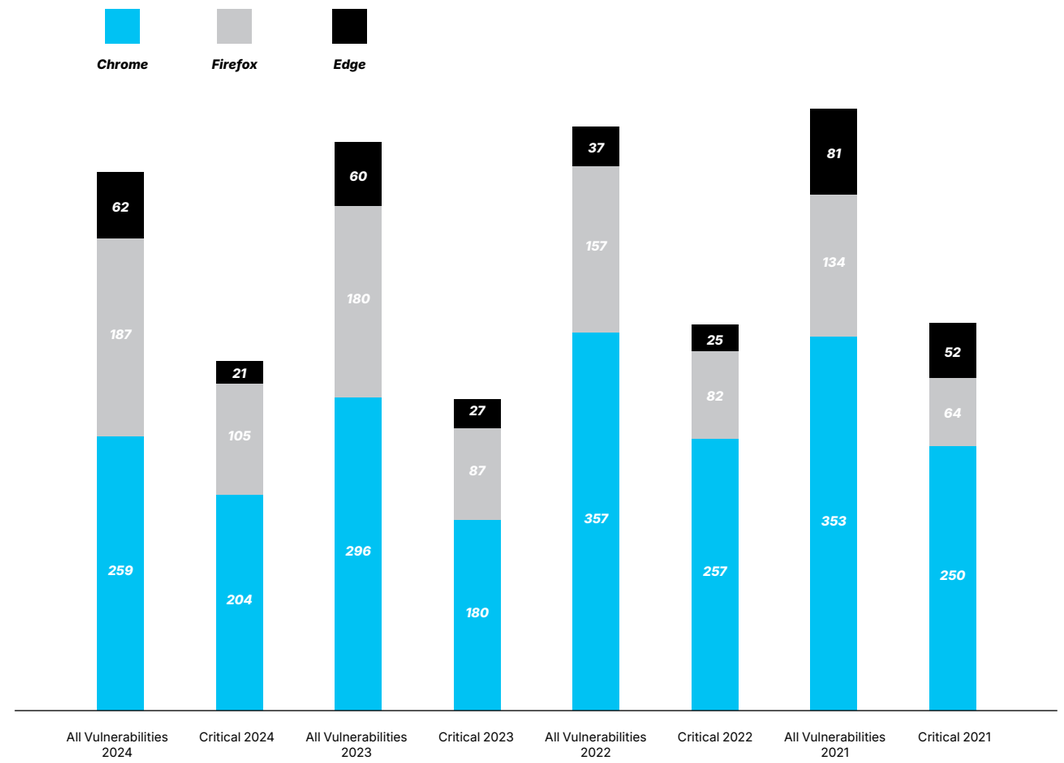
Edge: Rising RCE Threats

Microsoft Edge saw a notable drop in total vulnerabilities in 2022 (-54%), followed by an increase in 2023 (+62%) and a minor rise in 2024 (***+3%***). Critical vulnerabilities peaked in 2023 and declined in 2024 (***-22%***). However, RCE vulnerabilities showed a consistent upward trend, reaching 13 in 2024 (***+86%*** from 2023), indicating that while the overall count is relatively low, severity may be escalating. Exploited vulnerabilities remained low, with no change reported in 2024.

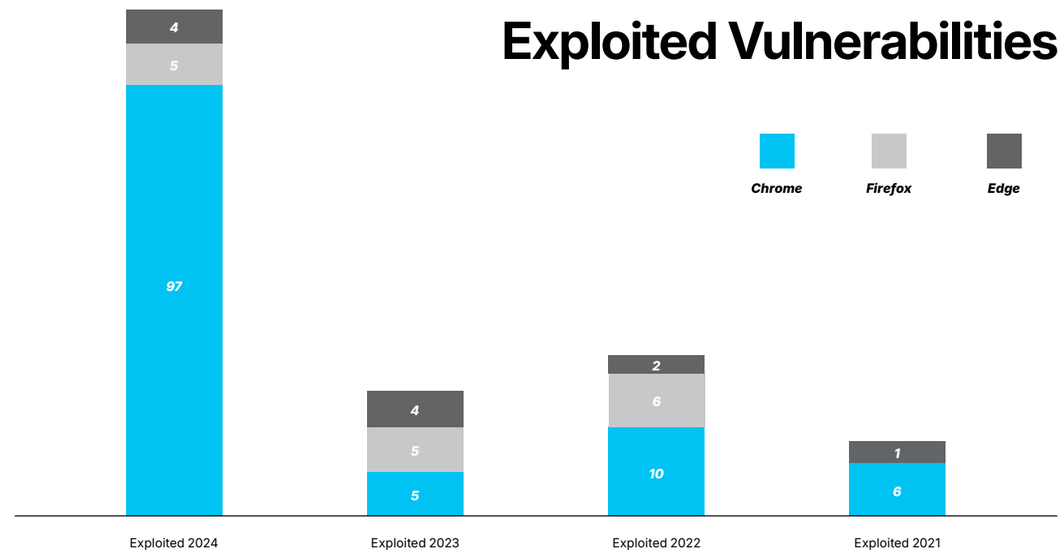
Escalating Critical and RCE Risks in Browsers

In summary, ***Firefox*** and ***Chrome*** both experienced increases in critical vulnerabilities in 2024, pointing to emerging security challenges that may demand closer attention. This rise could indicate that attackers or researchers are uncovering more severe flaws in these browsers. Additionally, the uptick in RCE vulnerabilities in ***Chrome*** and ***Edge*** highlights a potential rise in exploitability risks that should be closely monitored.

Total and Critical Vulnerabilities



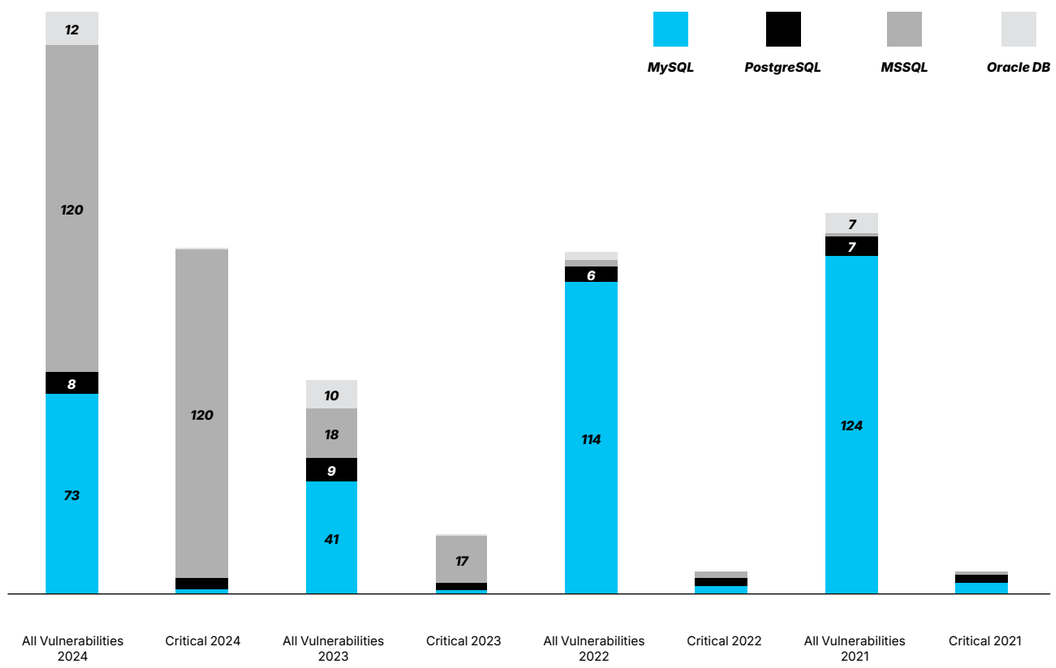
Exploited Vulnerabilities



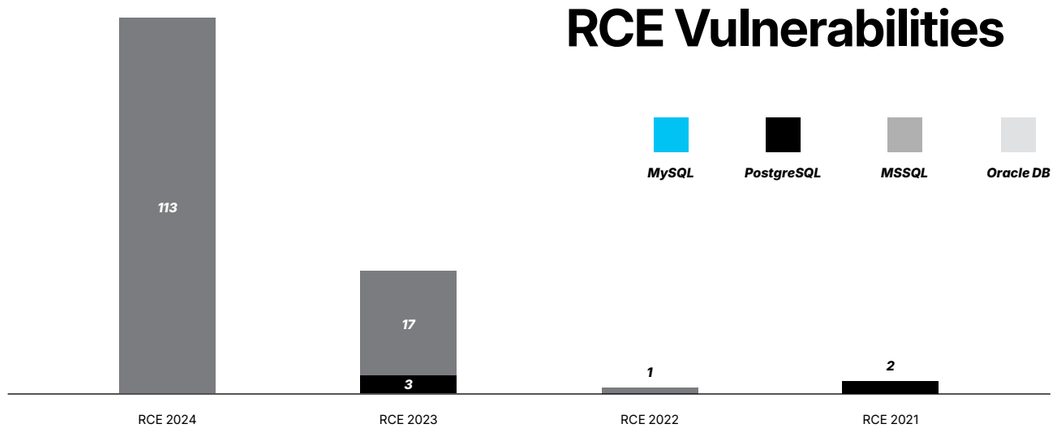
DATABASES

Name	AllVulnerabilities2024	Critical2024	RCE2024	AllVulnerabilities2023	Critical2023	RCE2023	AllVulnerabilities2022	Critical2022	RCE2022	AllVulnerabilities2021	Critical2021	RCE2021
MySQL	*73*	*2 +100%*	*0*	*41*	*1*	*0*	*114*	*3*	*0*	*124*	*4*	*0*
PostgreSQL	*8*	*4*	*0 -100%*	*9*	*3*	*3*	*6*	*3*	*0*	*7*	*3*	*2*
MSSQL	*120 +567%*	*120 +606%*	*113 +565%*	*18*	*17*	*17*	*2*	*2*	*1*	*1*	*1*	*0*
Oracle DB	*12*	*1*	*0*	*10*	*1*	*0*	*3*	*0*	*0*	*7*	*0*	*0*

Total and Critical Vulnerabilities



RCE Vulnerabilities



Overview

MSSQL: Escalating Risk

MSSQL saw a dramatic increase in total vulnerabilities, rising from only 1 in 2021 to ***120*** in 2024. Critical vulnerabilities also increased from 1 in 2021 to ***120*** in 2024. RCE vulnerabilities jumped from 0 in 2021 to ***113*** in 2024, highlighting a significant rise in reported issues.

The sharp increase in vulnerabilities, especially critical and RCE types, suggests that MSSQL has become a more attractive target for attackers. Organizations using MSSQL should prioritize patch management to mitigate potential threats.

MySQL: Volatile Vulnerability Trends

MySQL showed fluctuating vulnerability trends, with a 64% decrease from 2022 to 2023, followed by a ***78%*** increase from 2023 to 2024. Critical vulnerabilities remained low throughout the years.

This sharp decrease, followed by a subsequent rise, may reflect changes in security practices, updates to the codebase, or variation in detection efforts. With most vulnerabilities being of moderate severity, consistent monitoring remains essential to prevent potential escalation.

> Both ***MSSQL*** and ***MySQL***—despite a high number of vulnerabilities—had no reported exploited vulnerabilities in 2024. This could suggest effective patching or that vulnerabilities are discovered and addressed before attackers can exploit them.

Key Trends in PostgreSQL and Oracle Database

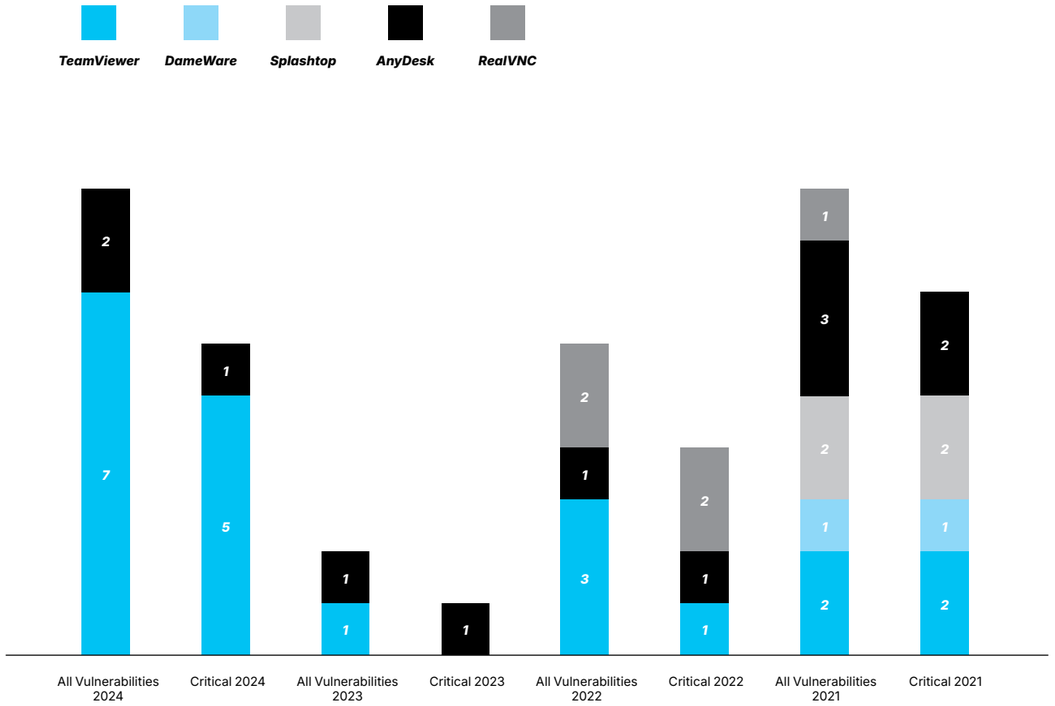
PostgreSQL maintained relative stability, with total vulnerabilities fluctuating slightly—a decrease in 2022 followed by minor year-over-year changes. Critical vulnerabilities remained consistently low, ranging from 3 to 4. RCE vulnerabilities appeared only in 2023. This stable and low vulnerability count may suggest effective security measures or less interest from attackers.

Oracle Database experienced a drop in total vulnerabilities in 2022, followed by increases in later years. Critical vulnerabilities remained minimal, with only one reported in both 2023 and 2024. While low numbers of critical vulnerabilities may reduce immediate risk, they do not eliminate the need for security due diligence.

REMOTE MANAGEMENT SOFTWARE

Name	AllVulnerabilities2024	Critical2024	Exploited2024	AllVulnerabilities2023	Critical2023	Exploited2023	AllVulnerabilities2022	Critical2022	Exploited2022	AllVulnerabilities2021	Critical2021	Exploited2021
TeamViewer	*7* *+600%*	*5*	*1*	*1*	*0*	*0*	*3*	*1*	*0*	*2*	*2*	*0*
DameWare	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*1*	*1*	*0*
Splashtop	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*2*	*2*	*0*
AnyDesk	*2* *+100%*	*1*	*1*	*1*	*1*	*0*	*1*	*1*	*0*	*3*	*2*	*0*
RealVNC	*0*	*0*	*0*	*0*	*0*	*0*	*2*	*2*	*0*	*1*	*0*	*0*

Total and Critical Vulnerabilities



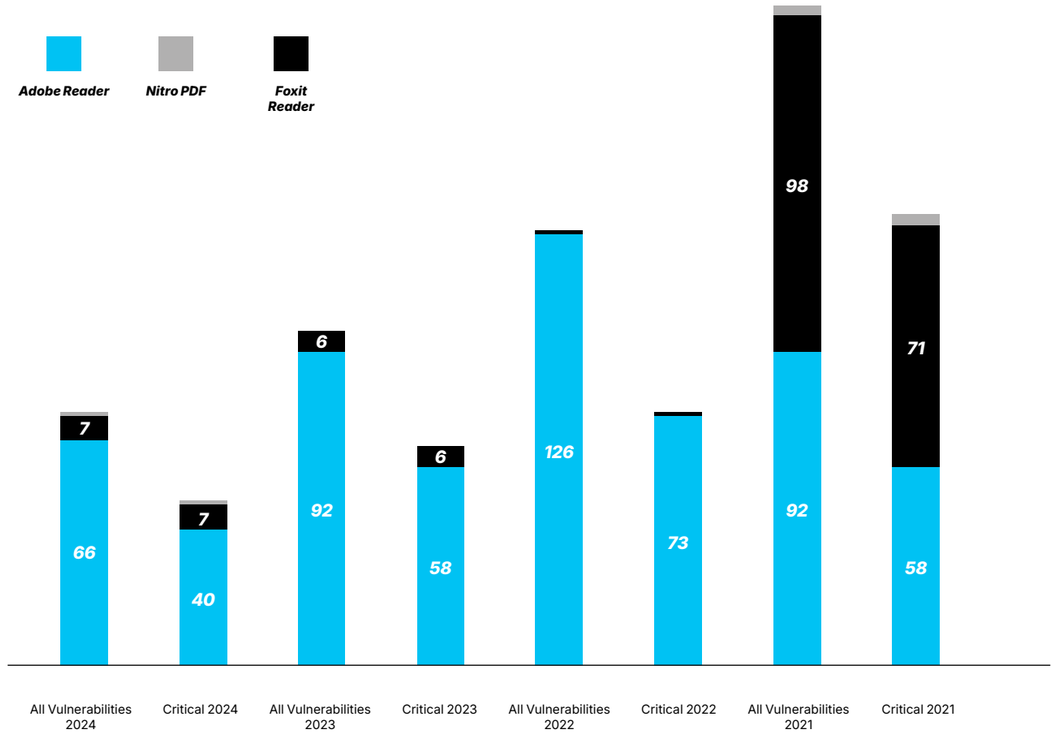
Overview

- ***TeamViewer*** experienced a resurgence in vulnerabilities, with a sharp ***increase in total cases*** in 2024 following a decline in 2023. Critical vulnerabilities also rose significantly in 2024, with ***five*** reported. This rise, especially in critical vulnerabilities, highlights potential security gaps. An exploited vulnerability was also reported in 2024—the first since 2020—indicating that attackers have resumed targeting the platform. The exploitation rate climbed from 0% in previous years to ***7.7%*** in 2024.
- ***AnyDesk*** vulnerability trends were inconsistent, with a decrease from 2021 to 2022, relative stability in 2023, and an ***increase*** in 2024—though still below 2021 levels. In 2024, ***AnyDesk*** reported its first exploited vulnerability in several years, pointing to increased attention from threat actors. The exploitation rate reached ***14.3%***, which is notable considering the small number of total vulnerabilities.
- ***DameWare*** and ***Splashtop*** reported ***no new vulnerabilities*** from 2022 to 2024. RealVNC saw its total vulnerabilities double in 2022 compared to 2021, followed by a ***drop to zero*** in both 2023 and 2024. This absence of new reports may reflect reduced focus by researchers and attackers, or potentially underreporting or insufficient auditing efforts.

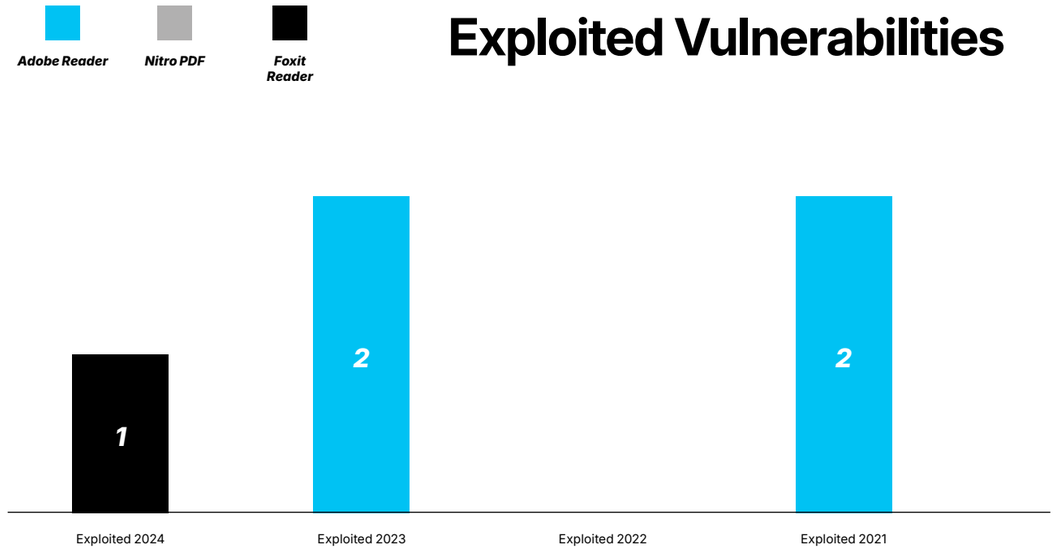
PDF READERS

Name	AllVulnerabilities2024	Critical2024	RCE2024	AllVulnerabilities2023	Critical2023	RCE2023	AllVulnerabilities2022	Critical2022	RCE2022	AllVulnerabilities2021	Critical2021	RCE2021
Adobe Reader	*66*	*40*	*3*	*92*	*58*	*3*	*126*	*73*	*10*	*92*	*58*	*1*
Foxit Reader	*7*	*7*	*0* *-100%*	*6*	*6*	*1*	*1*	*1*	*0*	*98*	*71*	*63*
Nitro PDF	*1*	*1*	*0*	*0*	*0*	*0*	*0*	*0*	*0*	*3*	*3*	*0*

Total and Critical Vulnerabilities



Exploited Vulnerabilities

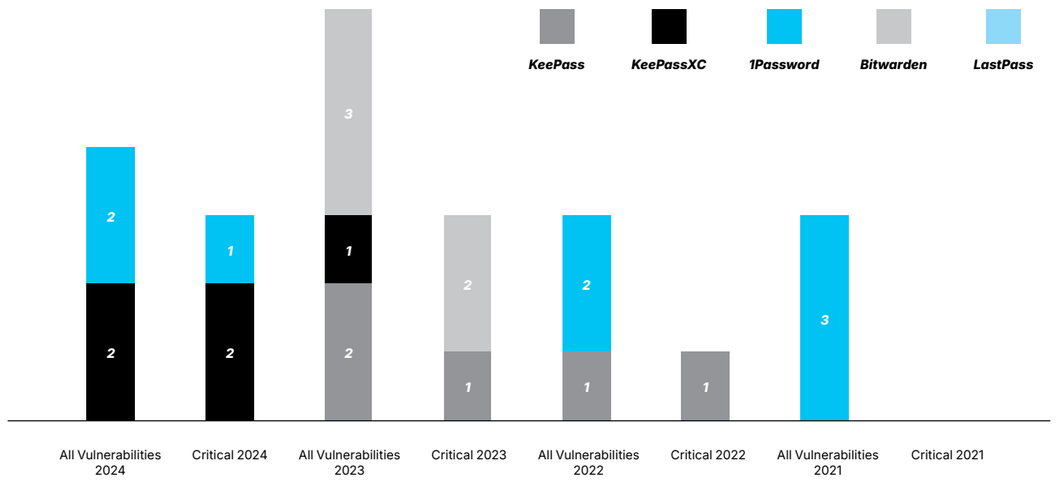


Overview

- ***Adobe Reader*** has shown a ***consistent decline*** in the number of vulnerabilities. After peaking in 2022, the total number of reported issues dropped significantly over the next two years. Critical vulnerabilities followed a similar downward trend. Exploited vulnerabilities, which reappeared in 2023, were eliminated again in 2024. This steady decline in both total and critical vulnerabilities suggests effective remediation efforts and strengthened security measures. However, the ***persistence of RCE vulnerabilities*** points to ongoing risks that still require attention. The ***elimination of exploited vulnerabilities*** in 2024 is a notable improvement and may reflect better patch adoption or enhanced security practices.
- ***Foxit Reader*** experienced a dramatic reduction in total vulnerabilities from 2021 to 2022 (–99%), followed by a sharp increase in 2023 and a ***moderate rise*** in 2024. Critical vulnerabilities mirrored this trend, suggesting volatility in security posture or reporting activity. An ***exploited vulnerability*** was recorded for ***the first time*** in 2024. These sharp fluctuations in vulnerability numbers may indicate instability in security processes or changing levels of scrutiny from researchers. The reappearance of vulnerabilities after a near-total drop in 2022 raises concerns about possible security lapses or inconsistencies in reporting practices.
- ***Nitro PDF*** had no reported vulnerabilities in 2022 and 2023, with ***one critical vulnerability*** surfacing in 2024. There were no exploited vulnerabilities reported during this period. The sudden appearance of a critical issue underscores that no software is entirely immune to risk—even those with a clean record can develop serious flaws. In ***Nitro PDF***'s case, however, this trend likely reflects a lack of popularity or scrutiny, rather than a robust security development lifecycle.

PASSWORD MANAGERS

Name	AllVulnerabilities2024	Critical2024	AllVulnerabilities2023	Critical2023	AllVulnerabilities2022	Critical2022	AllVulnerabilities2021	Critical2021
KeePass	***0*** *-100%*	***0*** *-100%*	***2***	***1***	***1***	***1***	***0***	***0***
KeePassXC	***2*** *+100%*	***2***	***1***	***0***	***0***	***0***	***0***	***0***
1Password	***2***	***1***	***0***	***0***	***2***	***0***	***3***	***0***
Bitwarden	***0*** *-100%*	***0*** *-100%*	***3***	***2***	***0***	***0***	***0***	***0***
LastPass	***0***	***0***	***0***	***0***	***0***	***0***	***0***	***0***



Overview

The ***total number of vulnerabilities*** for all password managers remains relatively low compared to other software categories, with only ***four in 2024***.

- ***KeePass*** reported ***zero vulnerabilities*** in 2024, after recording two in both 2022 and 2023. This reduction suggests successful remediation efforts and possibly strengthened security measures.
- ***KeePassXC*** saw an increase from zero critical vulnerabilities in previous years to ***two*** in 2024. This rise warrants attention to understand and address the underlying causes.
- After reporting zero vulnerabilities in 2023, ***1Password*** recorded ***two vulnerabilities*** in 2024. This marks a reemergence of risks that had previously been mitigated. The return of vulnerabilities may reflect new features or changes that introduced unforeseen risks.
- ***Bitwarden*** reported zero vulnerabilities in 2021 and 2022, a spike to three in 2023, and then returned to ***zero*** in 2024.
- ***LastPass*** reported ***no vulnerabilities*** from 2021 to 2024. However, it's important to consider external factors or security incidents (such as breaches) that may not be reflected in public vulnerability counts. This is particularly notable given ***LastPass*** has experienced several breaches in its history, most recently in 2024.

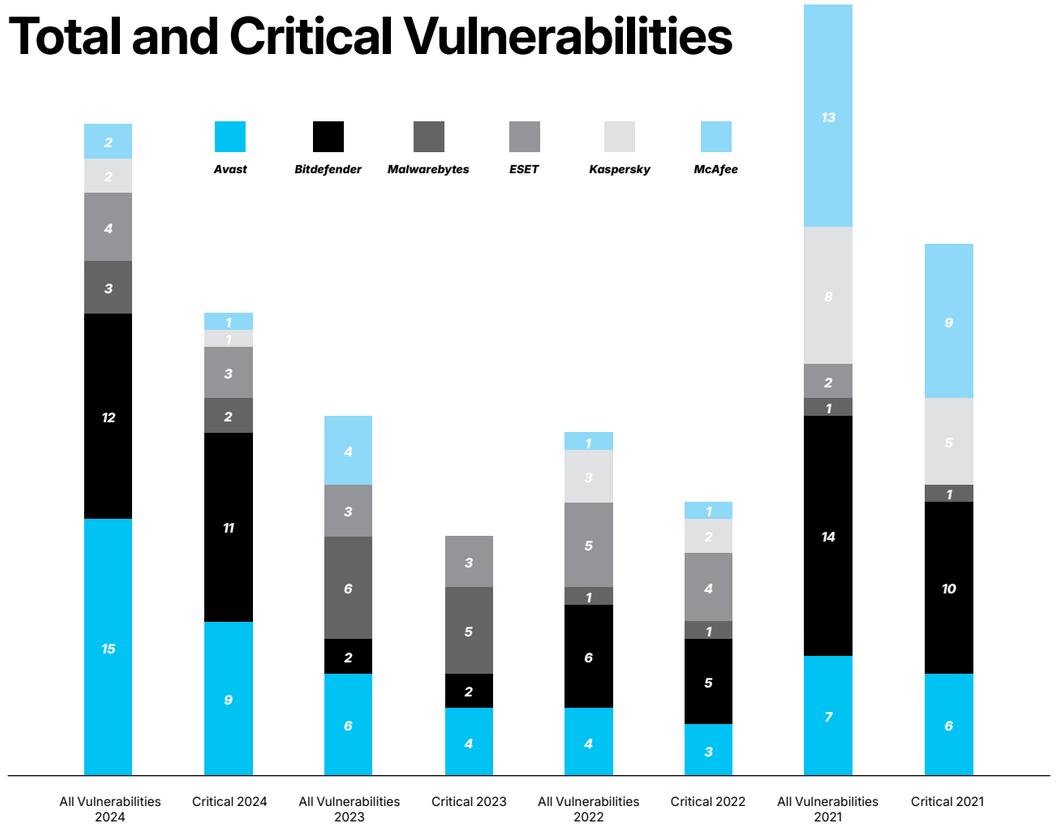
No exploited vulnerabilities were reported for any of the password managers across all years. The 0% exploitation rate suggests that while some vulnerabilities were disclosed, none were known to have been actively exploited, possibly due to effective mitigation measures or limited attacker interest.

Overall, the 2021–2024 data reflects a relatively resilient security posture in the password manager category, marked by consistently low vulnerability volumes and no confirmed exploitation.

ANTIVIRUS SOFTWARE

Name	AllVulnerabilities2024	Critical2024	RCE2024	AllVulnerabilities2023	Critical2023	RCE2023	AllVulnerabilities2022	Critical2022	RCE2022	AllVulnerabilities2021	Critical2021	RCE2021
Avast	***15*** ***+150%***	***9*** ***+125%***	***8***	***6***	***4***	***0***	***4***	***3***	***1***	***7***	***6***	***0***
Bitdefender	***12*** ***+500%***	***11*** ***+450%***	***1***	***2***	***2***	***0***	***6***	***5***	***0***	***14***	***10***	***3***
Malware-bytes	***3***	***2***	***3***	***6***	***5***	***0***	***1***	***1***	***0***	***1***	***1***	***0***
ESET	***4***	***3***	***0***	***3***	***3***	***0***	***5***	***4***	***0***	***2***	***0***	***0***
Kaspersky	***2***	***1***	***0***	***0***	***0***	***0***	***3***	***2***	***1***	***8***	***5***	***0***
McAfee	***2***	***1***	***0***	***4***	***0***	***0***	***1***	***1***	***1***	***13***	***9***	***1***

Total and Critical Vulnerabilities



Overview

- ***Total and Critical Vulnerabilities: Avast*** and ***Bitdefender*** experienced significant increases in total and critical vulnerabilities in 2024. ***McAfee***, ***ESET***, and ***Malwarebytes*** showed year-to-year variability with no consistent trend.
- ***RCE and Exploits: Avast*** and ***Malwarebytes*** reported ***RCE*** vulnerabilities in 2024—a notable development after previously reporting none. There were ***no exploited vulnerabilities*** reported across any product during the entire period.

The increase in vulnerabilities, particularly ***critical*** ones, in ***Avast (+150%)*** and ***Bitdefender (+500%)***, suggests growing software complexity or the introduction of new features that expand the attack surface. The emergence of ***RCE*** vulnerabilities in ***Avast*** and ***Malwarebytes*** is significant, given their potentially severe impact. ***Avast***, for instance, reported ***8 RCE*** vulnerabilities in 2024, up from none in previous years.

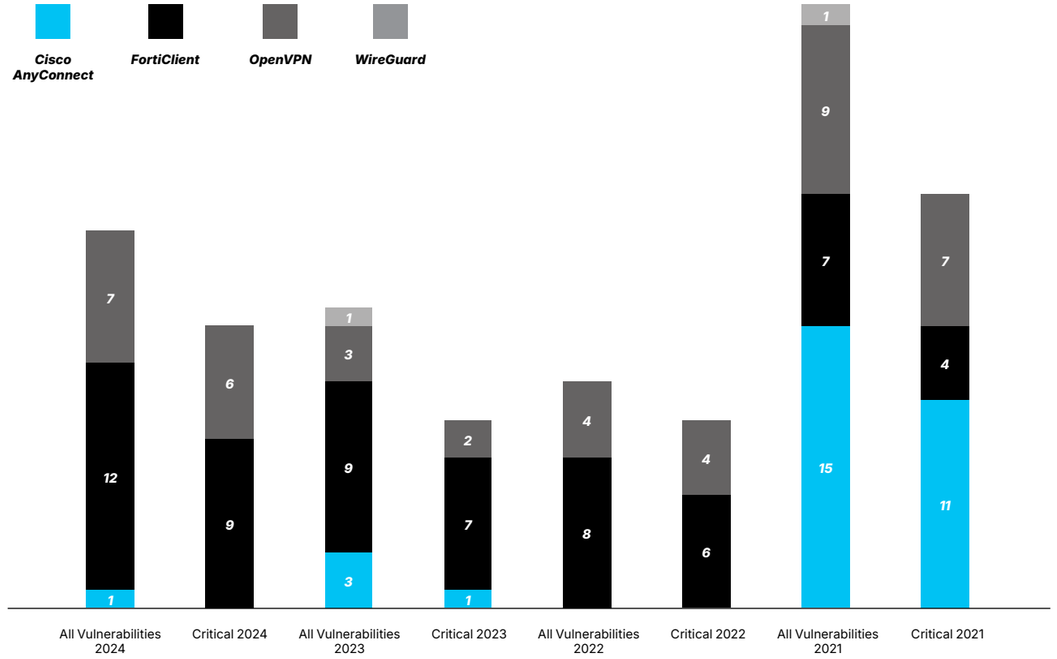
The consistent absence of exploited vulnerabilities points to effective mitigation strategies or a lack of focus by attackers on these products. The divergent trends among antivirus vendors likely reflect differences in development practices, security priorities, or market presence.

While the rise in vulnerabilities within antivirus software may challenge perceptions of their inherent security, the lack of exploitation activity—last seen in McAfee in 2021—indicates that attackers may be targeting more profitable or accessible vulnerabilities or facing stronger defenses.

VPN CLIENTS

Name	AllVulnerabilities2024	Critical2024	RCE2024	AllVulnerabilities2023	Critical2023	RCE2023	AllVulnerabilities2022	Critical2022	RCE2022	AllVulnerabilities2021	Critical2021	RCE2021
Cisco AnyConnect	***1***	***0*** -100%	***0*** -100%	***3***	***1***	***1***	***0***	***0***	***0***	***15***	***11***	***11***
FortiClient	***12***	***9***	***2***	***9***	***7***	***0***	***8***	***6***	***1***	***7***	***4***	***0***
OpenVPN	***7*** +133%	***6*** +200%	***3***	***3***	***2***	***0***	***4***	***4***	***0***	***9***	***7***	***0***
WireGuard	***0*** -100%	***0***	***0***	***1***	***0***	***0***	***0***	***0***	***0***	***1***	***0***	***0***

Total and Critical Vulnerabilities



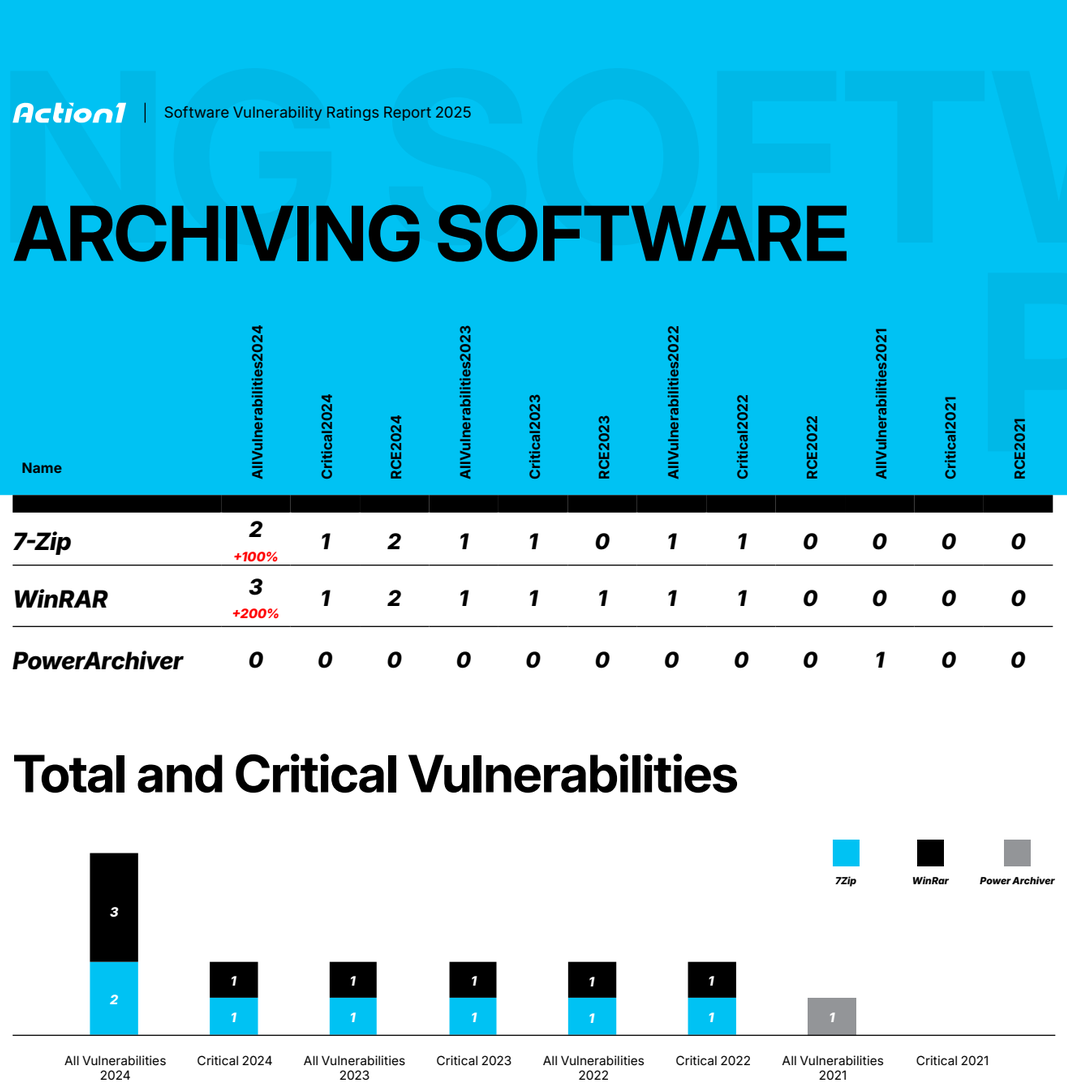
Overview

- ***Cisco AnyConnect*** experienced a significant decrease in total vulnerabilities, dropping from 15 in 2021 to just ***1 in 2024***. Critical vulnerabilities followed the same trend. This sharp decline across all types of vulnerabilities may indicate effective security measures or reduced software usage, leading to diminished interest from attackers and researchers.
- ***FortiClient*** showed a steady increase in total vulnerabilities over the four years, reaching 12 in 2024 (+33% from 2023)—the highest number among all VPN clients. It is also the only VPN client with ***a reported exploited vulnerability***. Critical vulnerabilities rose in parallel, reaching ***9 in 2024***. ***RCE*** vulnerabilities ***reappeared*** in 2024 after being absent in 2023. This consistent upward trend in both total and critical vulnerabilities highlights potential security challenges. Notably, Fortinet products have become a key target for attackers over the past two years.
- ***OpenVPN*** saw a decline in total vulnerabilities from 2021 to 2023, followed by a ***133%*** spike in 2024. Critical vulnerabilities mirrored this trend, rising by ***200%*** in the same year. ***RCE*** vulnerabilities also ***appeared for the first time*** in 2024, which could impact the platform's perceived security.
- ***WireGuard*** has consistently maintained a low vulnerability count, with ***zero reported*** in both 2022 and 2024. This likely reflects limited interest from threat actors, as the software is open-source and not widely adopted by large enterprises.

ARCHIVING SOFTWARE

Name	AllVulnerabilities2024	Critical2024	RCE2024	AllVulnerabilities2023	Critical2023	RCE2023	AllVulnerabilities2022	Critical2022	RCE2022	AllVulnerabilities2021	Critical2021	RCE2021
7-Zip	2 +100%	1	2	1	1	0	1	1	0	0	0	0
WinRAR	3 +200%	1	2	1	1	1	1	1	0	0	0	0
PowerArchiver	0	0	0	0	0	0	0	0	0	1	0	0

Total and Critical Vulnerabilities



Overview

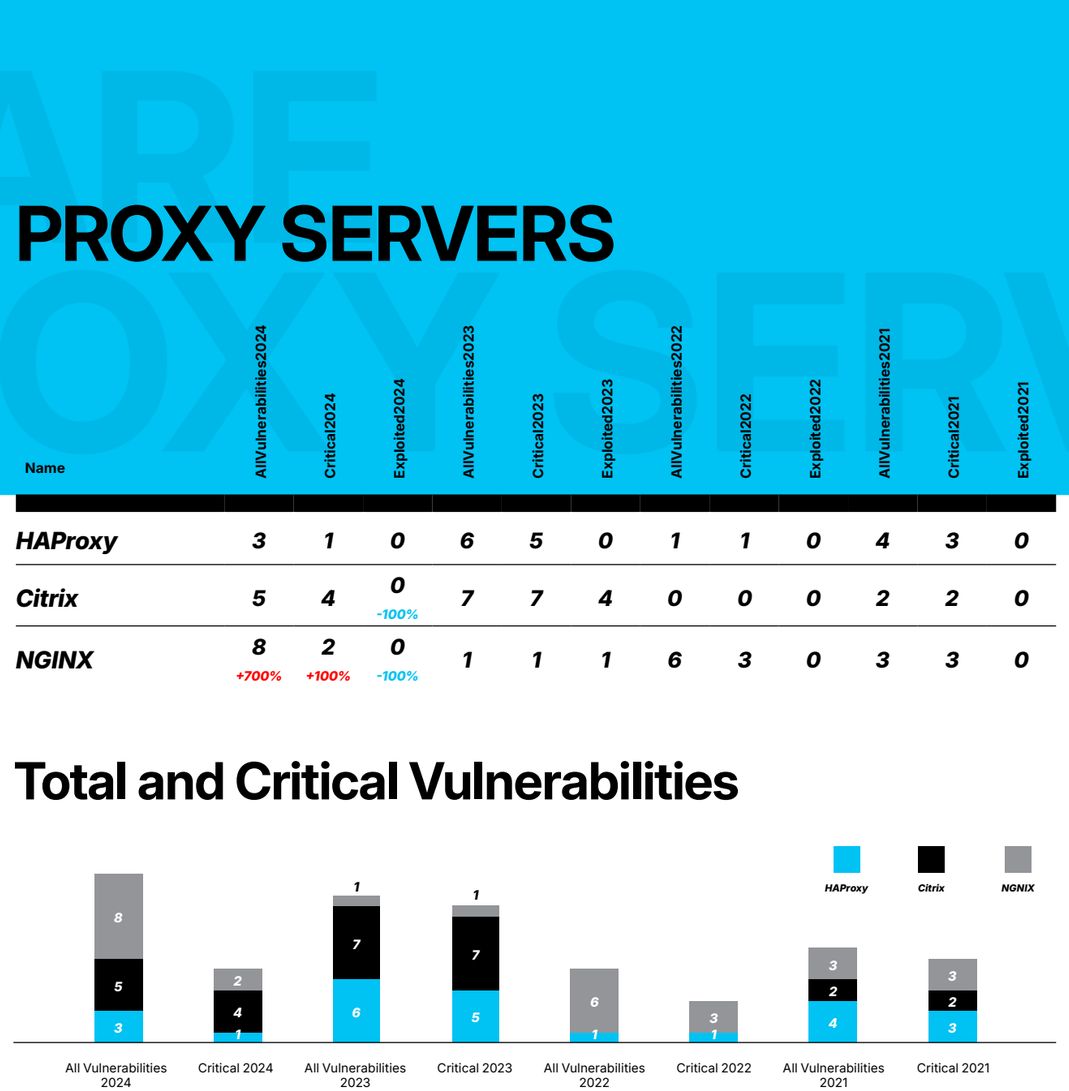
- The total number of vulnerabilities in ***7-Zip*** doubled from 1 in 2023 to ***2 in 2024***, while critical vulnerabilities remained steady at one from 2022 to 2024. Notably ***RCE*** vulnerabilities increased from 0 to ***2 in 2024***. This is significant, as RCE flaws allow attackers to remotely execute arbitrary code when a victim opens a malicious archive, posing a serious security risk. Additionally, 7-Zip reported its ***first exploited vulnerability*** in 2024, marking a shift in the focus of attackers. With 1 in 4 vulnerabilities exploited, the exploitation rate reached ***25%*** in 2024.
- ***WinRAR*** saw an increase in total vulnerabilities from 1 in 2023 to ***3 in 2024***. Critical vulnerabilities remained unchanged at one since 2022, while ***RCE*** vulnerabilities rose from 1 in 2023 to ***2 in 2024***. Despite this rise, no exploited vulnerabilities were reported in 2024 — a 100% decrease from the previous year.
- ***PowerArchiver*** reported a single moderate vulnerability in 2021 and ***none*** from 2022 to 2024. The absence of reported vulnerabilities may reflect lower usage or scrutiny, rather than strong security. A lack of disclosures does not necessarily indicate an absence of vulnerabilities—they may be undiscovered or unreported.

The simultaneous emergence of ***RCE*** vulnerabilities in both ***7-Zip*** and ***WinRAR*** in 2024 suggests a broader trend or shared weakness being targeted by attackers. This development may require cybersecurity professionals to re-evaluate threat models related to archiving software.

PROXY SERVERS

Name	AllVulnerabilities2024	Critical2024	Exploited2024	AllVulnerabilities2023	Critical2023	Exploited2023	AllVulnerabilities2022	Critical2022	Exploited2022	AllVulnerabilities2021	Critical2021	Exploited2021
HAProxy	3	1	0	6	5	0	1	1	0	4	3	0
Citrix	5	4	0 -100%	7	7	4	0	0	0	2	2	0
NGINX	8 +700%	2 +100%	0 -100%	1	1	1	6	3	0	3	3	0

Total and Critical Vulnerabilities



Overview

- ***HAProxy*** saw a sharp decrease in total vulnerabilities from 2021 to 2022 (-75%), followed by a significant spike in 2023 (+500%) and a subsequent decline in 2024 (***-50%***). Critical vulnerabilities followed a similar pattern, peaking in 2021 and 2023. Throughout the period, ***HAProxy*** reported no ***RCE or exploited vulnerabilities***, suggesting a relatively secure posture or lower prioritization by attackers.
- ***Citrix*** experienced a ***29%*** decrease in total vulnerabilities in 2024. Across the 2021-2024 period, ***13 out of 14*** reported vulnerabilities were classified as critical, highlighting the consistently high severity of issues discovered. ***One RCE*** vulnerability was reported in both 2023 and 2024. Notably, four ***exploited vulnerabilities*** tied to the CitrixBleed campaign were reported in 2023, dropping to ***zero*** in 2024—a clear sign that the campaign has ended and attackers have likely moved on to other targets.

- ***NGINX*** reported a rise in total vulnerabilities from 1 in 2023 to ***8 in 2024***, reversing the sharp decline seen the previous year. This surge may reflect increased scrutiny by researchers or newly discovered issues. However, it maintained ***zero RCE*** and ***zero exploited vulnerabilities*** throughout the entire four-year period.

Trends and Risk Evaluation

HAProxy and ***NGINX*** show notable year-over-year fluctuations in vulnerability counts, suggesting variability in either their underlying security posture or the level of researcher attention. They both reported ***zero RCEs*** over the four-year period. The ***absence of exploited vulnerabilities*** suggests a lower immediate risk, though continued vigilance remains essential. Given the critical role of proxy servers, this lack of exploitation is somewhat unexpected and may indicate stronger default security measures or a resilient architecture.

Citrix stands out with a ***higher overall severity*** profile and a recent history of active targeting. Although exploited vulnerabilities peaked during the CitrixBleed campaign in 2023 and none were reported in 2024, maintaining strong security practices remains essential when using this software.

RECOMMENDATIONS

The evolving vulnerability landscape requires organizations to stay vigilant, continuously monitor emerging threats, and adapt their security strategies to mitigate these risks. Based on our research, here are the key recommendations for improving security posture:

1. *Prioritize Critical Systems and Timely Patch Management.*

Operating systems, web browsers, and mobile platforms consistently exhibit high numbers of vulnerabilities, including critical and exploited ones. Organizations should prioritize patch management for these systems, dedicating resources to ensure they are updated quickly. Special attention should be given to software categories vulnerable to Remote Code Execution (RCE) attacks, such as desktop operating systems and databases, which require constant monitoring and rapid action to mitigate threats.

2. *Employee Education and Best Practices.*

Most vulnerabilities are exploited through specific actions by users. It's crucial to educate employees on the risks associated with common applications—especially Microsoft Office—emphasizing the importance of recognizing suspicious attachments and links. A proactive approach to safe browsing practices and timely patching can mitigate the risk of exploitation, particularly with web browsers.

3. *Comprehensive Vulnerability Management Across All Software.*

While this report focuses on specific categories of software, it highlights the need for CIOs and CISOs to apply a similar analysis across all software types used within their organization. This should encompass not only critical software like operating systems but also lesser-known tools (e.g., image editors, password managers) that might pose a security risk. This comprehensive approach is particularly important for software exposed to the internet or integral to business operations and sensitive data management.

4. *Third-Party Software Risk Assessment.*

When selecting third-party software, conduct a thorough risk assessment that evaluates not only the number of vulnerabilities but also their severity and the vendor's patch response time. While fewer vulnerabilities might suggest a more secure product, it's essential to consider the criticality of those vulnerabilities and the software's importance to your organization. Software with fewer vulnerabilities but slower patching or less robust mitigation strategies could present greater long-term risks.

5. *Continuous Threat Detection and Adaptability.*

A CISO must ensure that their organization has a dynamic security infrastructure that includes regular updates, robust threat detection, and the agility to adapt to emerging risks. Beyond addressing current vulnerabilities, anticipating future threats and adjusting security measures accordingly is key to maintaining a resilient security posture.