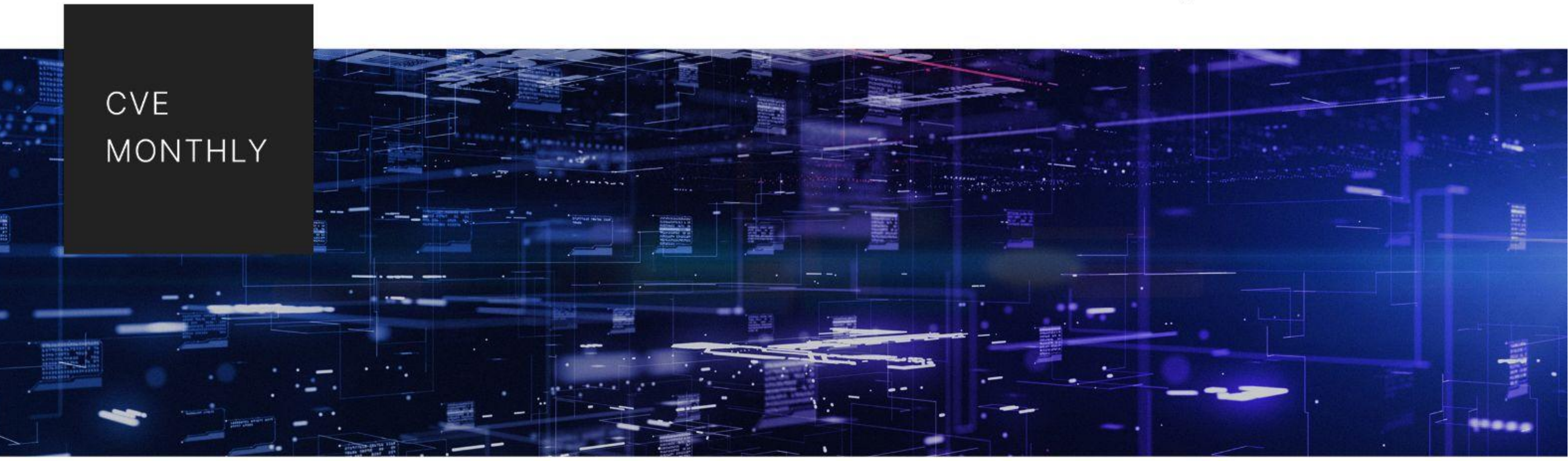
Recorded Future®



Recorded Future CVE Monthly January 2023

This report analyzes the top vulnerabilities disclosed across 8 major software vendors — Microsoft, Adobe, Oracle, Google, Apple, Apache, Linux, and Cisco — from January 1 to January 31, 2023. It includes the total number of vulnerabilities disclosed within the reporting period, the number of critical and zero-day vulnerabilities disclosed, the number of vulnerabilities actively exploited at the time of writing, and additional major trends and noteworthy vulnerabilities worth highlighting.

Key Judgments

- Recorded Future identified 11 newly disclosed vulnerabilities with high risk scores for January 2023 affecting Microsoft, only 1 of which is a zero-day vulnerability; at least 1 other (for SugarCRM) has also been exploited in the wild. The other vulnerabilities largely affect open-source software and routers from multiple vendors.
- 3 proof-of-concept (POC) exploits were released in January for end-of-life (EOL) Cisco routers, Zoho ManageEngine, and CentOS's Web Panel 7. For the latter 2 of these, publication of the POC exploit was followed shortly after or immediately by widespread exploitation.

CVE Monthly Prominent Vulnerability Disclosures

Talking about a "slow start" to the year feels disingenuous and inaccurate while thousands of organizations have faced ransomware compromise due to active exploitation of the ESXi vulnerability CVE-2021-21974. However, where January 2023 by itself is concerned, the beginning of the year has not only been fairly quiet for the vulnerability threat landscape, but has inverted the pattern of December 2022. In that month, several zero-day vulnerabilities affected 5 well-known vendors (Apple, Citrix, Fortinet, Google, and Microsoft). In January, on the other hand, we identified only 1 zero-day vulnerability, which affected Microsoft. Otherwise, many of the critical vulnerabilities that received press in January affected a small number of router firmware and open-source applications. The January developments that prompted the most attention weren't newly disclosed vulnerabilities — they were newly disclosed proof-of-concept (POC) exploits for previously disclosed vulnerabilities.

Researchers from Avast first discovered the aforementioned Microsoft zero-day vulnerability, CVE-2023-21674, which then appeared in Microsoft's Patch Tuesday list on January 10, 2023. Avast's discovery may foreshadow a longer blog from Avast about the vulnerability, but so far that has not yet appeared. The vulnerability allows elevation of privilege, specifically via browser sandbox escape, and mainly affects Windows Server 2012, although on social media Avast mentioned that it also affected "the latest Windows 10 and Windows 11 builds". Avast also claimed that the original exploit for CVE-2023-21674 was "most likely chained with a separate Chrome renderer RCE exploit" which they did not recover, so patching for this vulnerability should be a priority merely based on its existing in an exploit chain that security researchers have not sufficiently exposed.

The other newly disclosed and exploited vulnerability in our list was CVE-2023-22952, a flaw in several products from SugarCRM, a customer relationship management platform. In particular, the flaw affects the EmailTemplates module and can allow remote code execution (RCE). When first disclosed in January, it had a high CVSS score but no news of exploitation. On February 2, though, the US Cybersecurity and Infrastructure Security Agency (CISA) added CVE-2023-22952 to its list of known exploited vulnerabilities, immediately raising its criticality for defenders, particularly in the US where SugarCRM appears to have its largest customer base.

In the context of increasing package dependency attacks and abuse of cloud-based tooling, news of 2 RCE vulnerabilities in Git should prompt developer teams to be careful about how comfortably they clone external GitHub repositories. On January 17, 2023, security researchers from X41 and GitLab released a blog about how they had identified and patched 2 vulnerabilities as part of Git's security audit sponsored by the Open Source Technology Improvement Fund (OSTIF). The vulnerabilities, tracked as CVE-2022-41903 and CVE-2022-23521, were found in Git's commit-formatting mechanism and .gitattributes parser. The vulnerabilities affect Git versions 2.39 and older.

As mentioned, routers (including firmware and online interfaces) were a trending victim of critical vulnerabilities in January 2023, with affected devices coming from Netcomm (CVE-2022-4873), Cisco (CVE-2023-20025), and TP-Link (CVE-2023-22303). The Cisco vulnerability can present a unique challenge for defenders since Cisco has said in its advisory that it does not plan to release a patch for it — but this is perhaps less surprising since the affected router devices are either already outdated or received their last update as end-of-life (EOL) devices in late 2022. In the same advisory, Cisco noted that they were "aware that POC exploit code is available" for both CVE-2023-20025, which allows authentication bypass, and CVE-2023-20026, which allows remote code execution.

In the same category of POC exploits, 2 other vulnerabilities are worth mentioning for January: both exploits were published or identified in January, and both target vulnerabilities that were first disclosed in late 2022. On January 19, 2023, Rapid7 published a blog detailing their observation of exploitation activity involving a previously disclosed RCE vulnerability, tracked as CVE-2022-47966, which affects several Zoho ManageEngine products. The vulnerability was patched in November 2022. On the same day, the Horizon3 Team published a POC exploit for the vulnerability. Earlier, on January 13, 2023, the Horizon3 Team warned of "spray and pray" attacks targeting CVE-2022-47966. At the time, they also found more than 8,300 vulnerable ServiceDesk Plus and Endpoint Central instances. Similarly, a vulnerability in CentOS's Web Panel 7 reportedly received "mass exploitation" attempts after a POC exploit was published to GitHub on January 6, 2023.

Vulnerability	Risk Score	Vendor/ Product	Type of Component/ Software	Malware?	Zero-Day?
CVE-2023-21674	99	Microsoft Windows Server	Operating system		Yes
CVE-2023-22952	99	SugarCRM EmailTemplates	Email template creator		No
CVE-2022-4873	79	Netcomm NF20MESH, NF20, NL1902 Routers	Router firmware		No
CVE-2022-23521	79	Git .gitattributes	Git file format		No
CVE-2022-41903	79	Git commit-formatting	Git file format		No
CVE-2023-20025	79	Cisco Small Business RV042 Series Routers	Web-based interface		No

CVE-2023-21549	79	Microsoft Windows Server	Operating system		No
CVE-2023-22809	79	Sudo Project Sudo	Permissions and auditing application		No
CVE-2022-48198	78	Ntpd Driver	NTP memory driver		No
CVE-2023-22303	78	TP-Link SG105PE Firmware	Router firmware		No
CVE-2023-23488	75	WordPress Plugin “Paid Memberships”	Website plugin		No

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,500 businesses and government organizations across more than 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.