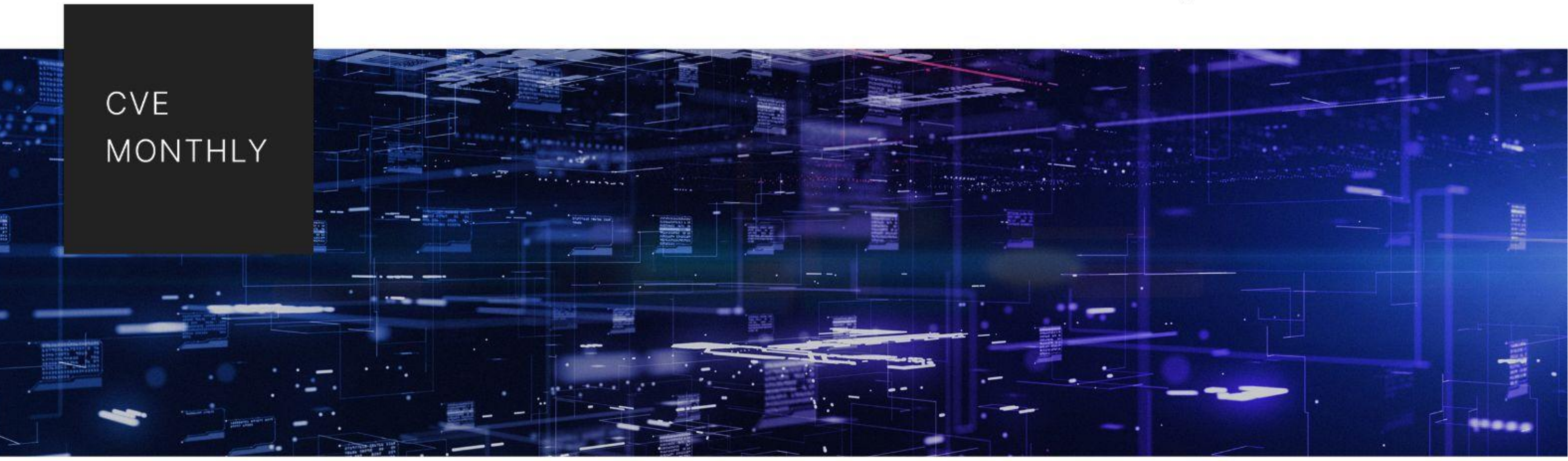

Recorded Future CVE Monthly February 2023

This report analyzes the top vulnerabilities disclosed across 8 major software vendors, including Microsoft, Adobe, Oracle, Google, Apple, Apache, Linux, and Cisco, from February 1 to February 28, 2023. This report 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 Findings

- Major software vendors disclosed 5 zero-day vulnerabilities in February 2023 that affect both consumer and enterprise products and software, including operating systems, graphics components, and desktop applications. These vulnerabilities affect products from Microsoft, Fortra, and Apple.
- Although some vulnerabilities had patches available, threat actors were still able to exploit vulnerabilities to launch widespread attacks against enterprise technology such as VMware ESXi servers.

CVE Monthly Prominent Vulnerability Disclosures

Although we tracked nearly the same amount of vulnerabilities this month as in January 2023, half of the listed vulnerabilities this month ran up scores of 99 in the Recorded Future Intelligence Cloud, meaning they had a score of "very critical". This number is higher when compared to January 2023, where just 2 of the vulnerabilities ranked with a score of 99.

Additionally, some of these February 2023 vulnerabilities were zero-days that affected widely-used technology products for both enterprises and consumers, which prompted companies to rapidly issue patches in the face of active exploitation. Consider the zero-day vulnerabilities below, which affected Apple, Microsoft, and Fortra products this month.

Apple released security updates on February 13, 2023, to address an actively exploited zero-day vulnerability in iPhone, iPad, and Mac devices. The vulnerability, tracked as CVE-2023-23529, is a WebKit type-confusion vulnerability that, if exploited, could execute arbitrary code on compromised devices, resulting in operating system crashes. CVE-2023-23529 is present in several Apple devices, including iPhone models after iPhone 8, all models of iPad Pro, iPad Air 3rd and 5th generation, iPad mini 5th generation, and Macs running macOS Ventura.

CVE-2023-23529 is Apple's first reported zero-day of 2023. Over the course of 2022, 4 of Apple's 10 patched zero-days were found in Apple's WebKit browser engine.

Microsoft also had 3 zero-day vulnerabilities known to be exploited in the wild, which affected components of its Windows ecosystem. The first vulnerability is a Windows Graphics Component remote code execution (RCE) vulnerability, tracked as CVE-2023-21823. The second is a Windows common log file system driver elevation of privilege vulnerability, tracked as CVE-2023-23376, which may allow an adversary to gain system privileges once successfully exploited. The last vulnerability is a Microsoft Publisher security features bypass vulnerability, tracked as CVE-2023-21715, which may allow an adversary to bypass Office macro policies that are used to block untrusted or malicious files in the targeted system.

The remaining zero-day vulnerability exploited this month belonged to **Fortra**. On February 7, 2023, Fortra released an updated patch for CVE-2023-0669, in its managed file transfer as a service (MFTaaS) product GoAnywhere MFT (Fortra is the cybersecurity and automation software company behind adversary emulation and red team tool, Cobalt Strike). The vulnerability allowed for RCE, but required access to the administrative console of the GoAnywhere MFT. The vulnerability could be exploited by threat actors on internet-facing instances of the GoAnywhere MFT administrative console. Indeed, Fortra's turnaround time between discovery of the GoAnywhere MFT vulnerability and releasing a patch for the vulnerability was relatively short: there was only 1 week between the vulnerability's public disclosure and a patch release. However, this quick fix did not keep the flaw from being exploited by threat actors: CISA added the vulnerability to its Known Exploited Vulnerabilities catalog on February 10, 2023.

While these vulnerabilities were both recently disclosed and exploited in February 2023, older, known vulnerabilities were also actively exploited — even if there was already a remediation available. Beginning on February 3, 2023, a ransomware outbreak targeted VMware ESXi hypervisor servers that would append infected files with the extension ".args" (ESXiArgs). The French Computer Emergency Response Team (CERT-FR) subsequently reported that the operators of ESXiArgs were likely exploiting CVE-2021-21974 to launch ransomware on the servers. CVE-2021-21974 is exploited by triggering a heap-overflow issue in an OpenSLP service, allowing for RCE; a patch for CVE-2021-21974 has been available since February 23, 2021.

In a follow-up security advisory, VMware stated that there was no evidence of threat actors exploiting zero-day vulnerabilities to attack servers. Rather, "most reports state that End of General Support (EOGS) and/or significantly out-of-date products are being targeted with known vulnerabilities which were previously addressed and disclosed in VMware Security Advisories". In other words, vulnerabilities like CVE-2021-21974 were fair game for threat actors.

Vulnerability	Risk Score	Vendor/ Product	Type of Component/ Software	Malware?	Zero-Day?
CVE-2023-23529	99	Apple WebKit	Browser engine		Yes
CVE-2023-21823	99	Microsoft Windows Server Graphic component	Operating system		Yes
CVE-2023-23376	99	Microsoft Windows Common Log File System	Log file API		Yes
CVE-2023-0669	99	Fortra GoAnywhere MFT	File transfer application		Yes
CVE-2023-21715	99	Microsoft Office Publisher	Desktop publishing application		Yes
CVE-2023-23969	99	Dell Data Domain Operating System	Operating system		No
CVE-2023-22501	79	Jira Service Management Server and Data Center	Ticket management application		No
CVE-2023-0286	79	OpenSSL x.400 command	Address types within multipurpose certificate utility		No
CVE-2023-25136	79	OpenSSH server	Secure communication daemon		No
CVE-2023-23692	78	Dell Data Domain Operating System	Operating system		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 1,400 businesses and government organizations across more than 60 countries.

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