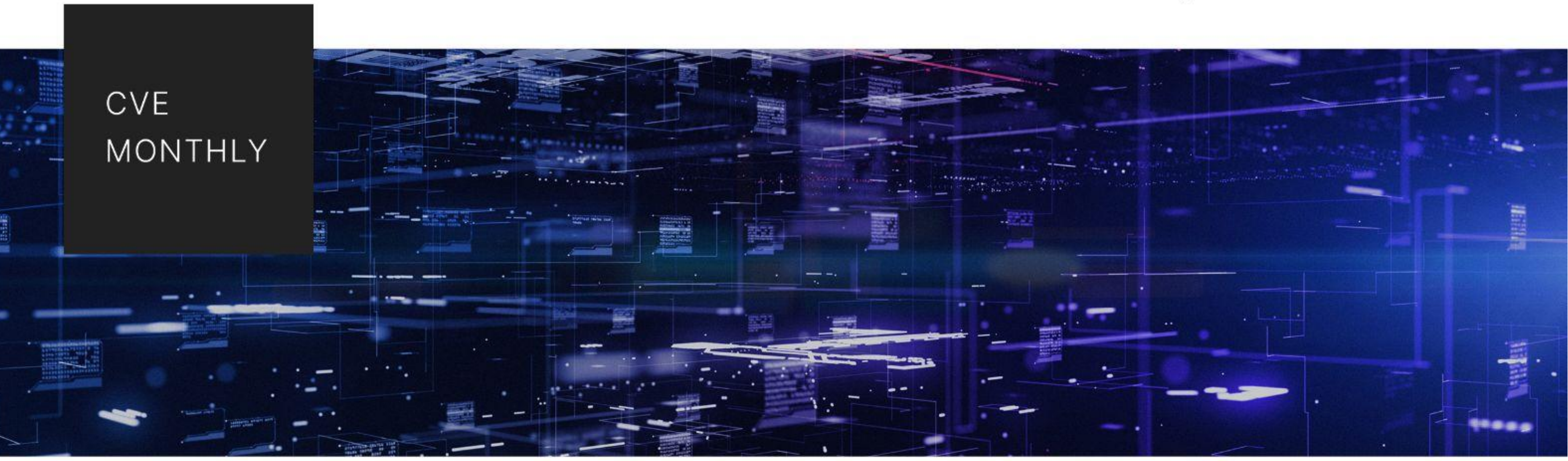
CVE
MONTHLY



Recorded Future CVE Monthly May 2023

This report analyzes the top vulnerabilities disclosed across 8 major software vendors — Microsoft, Adobe, Oracle, Google, Apple, Apache, Linux, and Cisco — from May 1 to May 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.

Key Findings

- 7 zero-day vulnerabilities in May 2023 affected Microsoft, Apple, Barracuda Networks, and Progress Software products.
- 16 of the approximately 2,400 vulnerabilities disclosed were high risk.
- Samsung Android devices were affected by a high-risk vulnerability that was confirmed to be actively exploited.
- 5 critical vulnerabilities associated with Cisco products were identified.

CVE Monthly Prominent Vulnerability Disclosures

We identified 16 newly disclosed vulnerabilities with high risk scores for May 2023, 7 of which are zero-day vulnerabilities affecting Microsoft, Apple, Barracuda Networks, and Progress Software products. The 3 vulnerabilities that attracted some of the highest attention from security researchers according to our dataset were CVE-2023-24932, a Secure Boot security feature bypass zero-day vulnerability affecting various versions of Microsoft Windows that has been actively exploited by the BlackLotus bootkit malware family; CVE-2023-34362, a SQL injection zero-day vulnerability in Progress Software's MOVEit Transfer file transfer solution; and CVE-2023-2868, a zero-day vulnerability affecting Barracuda's Email Security Gateway (ESG) appliance. All 3 of these vulnerabilities were actively exploited prior to the development of patches. For CVE-2023-2868, instances of exploitation accelerated after its disclosure.

Microsoft released security updates [1, 2] to address 2 actively exploited zero-day vulnerabilities affecting Microsoft Windows Server as part of its May 2023 Patch Tuesday. If exploited, the vulnerabilities (CVE-2023-24932 and CVE-2023-29336) can allow threat actors to bypass security features and elevate privileges on a targeted system, respectively. According to Microsoft's advisory for CVE-2023-24932, the flaw had been exploited by malicious actors to deploy the BlackLotus bootkit malware. BlackLotus has various persistence and defense evasion capabilities, including disabling security programs such as BitLocker, hypervisor-protected code integrity (HVCI), and Windows Defender.

On May 31, 2023, Progress Software released a patch for CVE-2023-34362, a SQL injection zero-day vulnerability in its MOVEit Transfer file transfer solution. If exploited, CVE-2023-34362 can allow an unauthenticated attacker to gain access to MOVEit Transfer's database. On June 1, 2023, Rapid7 reported that its managed services teams were observing the exploitation of CVE-2023-34362 after the vulnerability's disclosure. According to Mandiant's CTO, Charles Carmakal, Mandiant's records show that attacks involving the exploitation of the CVE-2023-34362 started on May 27, 2023. Carmakal advised affected organizations to "prepare for the potential extortion and publication of the stolen data". In its advisory, Progress Software instructed users to "disable all HTTP and HTTPS traffic to your MOVEit Transfer environment", "delete unauthorized files and user accounts and reset credentials", and "apply available patches".

The exploitation of vulnerabilities in file transfer services is a common way that threat actors gain access to corporate networks. The increased exploitation of CVE-2023-34362 after its disclosure prompted some to compare MOVEit Transfer to another file transfer service, Fortra's GoAnywhere managed file transfer (MFT), wondering whether it would suffer a similar fate. Despite being patched since February 2023, threat actors have been able to repeatedly exploit CVE-2023-0669, a vulnerability in the GoAnywhere MFT, to carry out successful, high-profile cyberattacks up to at least May 2023.

Barracuda Networks discovered CVE-2023-2868, a zero-day vulnerability in its Email Security Gateway (ESG) appliance (responsible for scanning incoming emails), on May 19, 2023. Barracuda Networks subsequently uncovered evidence that the vulnerability had been exploited since at least October 2022, long before it was patched on May 20, 2023. CVE-2023-2868 stems from incomplete input validation, and according to NIST it can enable remote execution of “a system command through Perl's qx operator with the privileges of the Email Security Gateway product”. CISA added CVE-2023-2868 to its catalog of Known Exploited Vulnerabilities (KEV) on May 26, 2023.

Apple patched 3 zero-day vulnerabilities affecting iPhones, Macs, and iPads on May 18, 2023. CVE-2023-32409, CVE-2023-28204, and CVE-2023-32373 all affect Apple’s WebKit browser engine, used on multiple Apple platforms. CVE-2023-32409 is a sandbox escape flaw that would allow a remote attacker to break out of Web Content sandbox; CVE-2023-28204 is an out-of-bounds read flaw that could allow access to sensitive content; and CVE-2023-32373 is a use-after-free flaw that could allow arbitrary code execution. In its advisory, Apple indicated that CVE-2023-32409, which was reported by Clément Lecigne of Google's Threat Analysis Group and Donncha Ó Cearbhaill of Amnesty International’s Security Lab, “may have been actively exploited in the wild”. Later, on May 22, 2023, US Cybersecurity and Infrastructure Agency (CISA) added all 3 vulnerabilities to its KEV Catalog, which confirmed they had been exploited on real-world devices. The vulnerabilities are not yet listed in the National Institute of Standards and Technology’s (NIST) National Vulnerability Database (NVD) as of the writing of this report.

Samsung Android 11, 12, and 13 devices were affected by CVE-2023-21492, a high-risk vulnerability disclosed in early May 2023. CVE-2023-21492 is an insertion of a sensitive information vulnerability that exists in a log file that could allow threat actors with privileged access to bypass the Android Address Space Layout Randomization (ASLR) protection. Threat actors could exploit the vulnerability to inject malicious code into processes, bypass process-based defenses, and potentially elevate privileges. Samsung disclosed in its May 2023 Security Maintenance Release (SMR) that exploit code for CVE-2023-21492 publicly existed. On May 19, 2023, CISA added CVE-2023-21492 to its KEV catalog, confirming it has been actively exploited on real-world devices.

Wordpress plugins were affected by 2 high-risk vulnerabilities in May, both of which were confirmed to have been actively exploited after their disclosure. Bleeping Computer reported on May 14, 2023, that threat actors were actively exploiting CVE-2023-30777, a high-severity reflected XSS flaw affecting Advanced Custom Fields that allows unauthenticated attackers to steal sensitive information and escalate privileges on affected WordPress sites. Additionally, Wordfence reported on May 17, 2023, that threat actors were actively exploiting CVE-2023-32243, a recently patched critical privilege escalation vulnerability found in the Essential Addons for Elementor plugin for WordPress. Security researchers published proof-of-concept exploit code for the vulnerability on Github on May 14, 2023. Subsequently, there were millions of probing attempts for the plugin present on websites, and approximately 6,900 exploitation attempts were blocked, as observed by Wordfence at the time of its report.

BleepingComputer reported on May 9, 2023, that Linux kernel NetFilter contained a privilege escalation vulnerability, tracked as CVE-2023-32233, that could allow an unauthenticated threat actor to gain root access and take over the affected system. On May 16, 2023, GitHub user Liuk3r published a proof-of-concept script for CVE-2023-32233 to allow a user to obtain root privileges.

The script has been tested on a machine running Ubuntu version 23.04 (Lunar Lobster). Liuk3r warned users that the script could corrupt the kernel memory of the vulnerable machine. However, as of writing this report, there is no evidence that CVE-2023-32233 has been actively exploited.

Finally, Cisco disclosed 5 high-risk vulnerabilities, 1 affecting its port phone adapter firmware (CVE-2023-20126) and 4 affecting small business smart and managed switches (CVE-2023-20189, CVE-2023-20161, CVE-2023-20160, CVE-2023-20159). While the vulnerabilities should be prioritized for remediation given their elevated risk scores, none of the vulnerabilities are confirmed to have been actively exploited.

Vulnerability	Risk Score	Vendor/ Product	Type of Component/ Software	Malware	Zero-Day
CVE-2023-29336	99	Microsoft	Windows servers and clients	BlackLotus, MysterySnail RAT	Yes
CVE-2023-24932	99	Microsoft	Windows servers and clients	BlackLotus	Yes
CVE-2023-32409	99	Apple	WebKit browser engine	N/A	Yes
CVE-2023-28204	99	Apple	WebKit browser engine	N/A	Yes
CVE-2023-32373	99	Apple	WebKit browser engine	N/A	Yes
CVE-2023-21492	99	Samsung	Android	Metasploit, Offensive Security Tools (OST)	No
CVE-2023-2868	99	Barracuda Networks	Email Security Gateway (ESG) appliance	N/A	Yes
CVE-2023-32243	99	WPDeveloper Essential Addons for Elementor	WordPress plugin	N/A	No
CVE-2023-30777	99	Advanced Custom Fields for WordPress	WordPress plugin	N/A	No
CVE-2023-34362	89	Progress Software MOVEit Transfer	File transfer software	N/A	Yes

Vulnerability	Risk Score	Vendor/ Product	Type of Component/ Software	Malware	Zero-Day
CVE-2023-32233	79	Linux NetFilter	Kernel	Metasploit, Traitor, OST, NetFilter	No
CVE-2023-20126	79	Cisco Spa112 Firmware	Firmware	N/A	No
CVE-2023-20189	77	Cisco Small Business Smart and Managed Switches	Switch	N/A	No
CVE-2023-20161	76	Cisco Small Business Smart and Managed Switches	Switch	N/A	No
CVE-2023-20160	76	Cisco Small Business Smart and Managed Switches	Switch	N/A	No
CVE-2023-20159	75	Cisco Small Business Smart and Managed Switches	Switch	N/A	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 1,600 businesses and government organizations across more than 70 countries.

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