Recorded Future®

CVE
MONTHLY

Recorded Future CVE Monthly April 2023

This report analyzes the top vulnerabilities disclosed across 8 major software vendors — Microsoft, Adobe, Oracle, Google, Apple, Apache, Linux, and Cisco — from April 1 to April 30, 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 Findings

- Major software vendors disclosed 7 zero-day vulnerabilities in April 2023 that affect both consumer and enterprise products and software, including security features, access control components, sandboxing environments, and operating systems.
- 15 of the approximately 2,200 vulnerabilities disclosed were high-risk.
- Microsoft's Windows operating system continues to see new vulnerability exploitation, as befits its high market share.
- Several critical vulnerabilities associated with VM2, a JavaScript sandboxing environment, were identified in the reporting period.

CVE Monthly Prominent Vulnerability Disclosures

We identified 15 newly disclosed vulnerabilities with high risk scores for April 2023, 6 of which are zero-day vulnerabilities affecting Microsoft, Apple, and Google. The 3 vulnerabilities that attracted some of the highest attention from security researchers according to our dataset were: CVE-2023-28252, an out-of-bounds write vulnerability in Windows Common Log File System; CVE-2023-2033, a type confusion vulnerability in Google Chrome's V8 Javascript engine; and CVE-2023-28206, an out-of-bounds write vulnerability in Apple's IOSurfaceAccelerator and WebKit. In CVE-2023-28252's case, the flaw has been exploited to ultimately deploy Nokoyawa ransomware payloads. The main trend affecting the non-major vendors were several critical vulnerabilities associated with VM2, a Javascript sandboxing environment.

Google issued 2 updates to address the Chrome vulnerability CVE-2023-2033 on April 14, 2023. The vulnerability is a type confusion weakness in Chrome's V8 Javascript engine that can be exploited by crafting HTML pages to trigger a heap overflow. Google stated that an exploit for the vulnerability exists in the wild, but did not specify whether this exploit was actively being used by threat actors. At the time of writing, the vulnerability does not have a CVSS score, since the vulnerability is still undergoing preliminary analysis. This vulnerability received the most attention in terms of references from security researchers this month, according to our data set on the Recorded Future Intelligence Cloud.

BleepingComputer reported that this is Google Chrome's first publicly reported vulnerability to have an exploit in the wild in 2023. Google recommends that users update their Chrome versions to 112.0.5615.121 to remediate the vulnerability. However, even if Chrome is configured to load automatic updates, users still need to relaunch their Chrome browser to implement the patch.

Microsoft, consistent with recent months, was once again the most prominent vendor, accounting for 3 high-risk vulnerabilities. First, on April 11, 2023, Microsoft disclosed a remote code execution (RCE) vulnerability tracked as CVE-2023-28311. A threat actor could execute arbitrary code on a system through the vulnerability in Microsoft Office if a victim opens a specially crafted file. This vulnerability can then be exploited to run unauthorized code on the system.

Second, Microsoft released a second advisory on April 11, 2023, regarding a zero-day vulnerability in the Windows Common Log File System (CLFS). The vulnerability, tracked as CVE-2023-28252, is an out-of-bounds write vulnerability that allows an authenticated threat actor to gain SYSTEM privileges. A threat actor could exploit the vulnerability by manipulating base log files. As a result, a threat actor could modify the registry contents of the *HKEY_LOCAL_MACHINE\SAM*, allowing for privilege escalation exploits and access to credentials. The affected products are all versions of Windows servers and clients. The vulnerability is currently being exploited in the wild for privilege escalation by the Nokoya ransomware group. Microsoft addressed CVE-2023-28252 as part of the April 2023 Microsoft Patch Tuesday.

Third, also on April 11, 2023, Check Point Research identified a vulnerability tracked as CVE-2023-21554 in Microsoft Message Queuing Service (MSMQ), which may allow arbitrary code execution and denial-of-service (DoS) of Windows service processes. “MSMQ is a messaging infrastructure and a development platform for creating distributed, loosely-coupled messaging applications for Windows operating systems”, as defined by Microsoft. The vulnerability was immediately patched and addressed after discovery. CVE-2023-21554, also known as QueueJumper, is a critical vulnerability. Once exploitation of CVE-2023-21554 occurs, adversaries can perform unauthorized RCE on the Microsoft Message Queuing Service via TCP port 1801.

Apple was also a prominent vendor in this month’s data set. Apple vulnerabilities accounted for 2 of the vulnerabilities with very critical risk scores: CVE-2023-28205 and CVE-2023-28206. Apple released security updates on April 7, 2023, to address these 2 zero-day vulnerabilities in Apple iOS, iPadOS, Safari WebKit, and MacOS Ventura versions before 13.3.1. The first vulnerability, CVE-2023-28205, is a use-after-free vulnerability that if exploited can lead to code execution when processing malicious web content. The second vulnerability, CVE-2023-28206, is an out-of-bounds write vulnerability in IOSurfaceAccelerator and WebKit that could lead to data corruption, system crash, and code execution with kernel privileges. A threat actor could exploit CVE-2023-28206 via specially crafted web content. Apple addressed the vulnerabilities with a patch for improved input validation and memory management.

Clément Lecigne of Google's Threat Analysis Group and Donncha Ó Cearbhaill of Amnesty International's Security Lab initially reported the 2 Apple vulnerabilities. In a statement to Dark Reading, a technical engineer from cyber security company Vulcan Cyber commented that the involvement of Amnesty International indicates the flaws are being exploited by nation-state actors. The engineer stated: "While Apple hasn't said much about the exploits, it seems likely, given the reporting and earlier history, that the exploits were deployed by state-level threat actors". Apple protects users by not disclosing technical details about zero-day vulnerabilities, in order to slow threat actors’ ability to develop and deploy new exploits that target vulnerable devices.

On April 18, 2023, Google rolled out security updates to address a Google Chrome high-severity zero-day vulnerability tracked as CVE-2023-2136. The vulnerability is an integer overflow flaw in Skia, an open-source 2D graphics library in Google Chrome that allows a remote attacker to compromise the renderer process to potentially perform a sandbox escape via a crafted HTML page. An integer overflow vulnerability occurs when an operation result exceeds the maximum value for a given integer type. In Skia's case, the integer overflow might lead to incorrect rendering, memory corruption, and arbitrary code execution that may lead to unauthorized system access. Google has not disclosed details about how the vulnerability is being used in attacks.

A further vulnerability with a very critical risk score affecting products of a major software vendor this month was CVE-2023-27350. Microsoft reported on April 27, 2023, regarding a DEV-0950 (Lace Tempest) campaign exploiting recently discovered vulnerabilities in the PaperCut Multifunction (MF) and Next Generation (NG) software to deliver LockBit and Clop Ransomware. The vulnerability, tracked as CVE-2023-27350, "could allow unauthenticated remote attackers to achieve arbitrary code execution and gain unauthorized access to sensitive information" on compromised PaperCut software installations.

In the context of vulnerabilities pertaining to open-source software modules outside of the major vendors discussed, the Javascript sandboxing environment VM2 library was a trending victim of critical vulnerabilities in March 2023. The following vulnerabilities, tracked as CVE-2023-29199, CVE-2023-30547, and CVE-2023-29017, affect the popular VM2 library, a JavaScript sandbox used for running code securely in a virtualized environment. On April 17, 2023, a security researcher published a proof of concept (PoC) exploit for CVE-2023-30547, a vulnerability affecting VM2 sandbox that allows for malicious code to escape a VM2 sandbox instance by manipulating the handleException() function. A POC exploit code was made available for a vulnerability, tracked as CVE-2023-29017, which has a maximum severity score of 10.0 and was discovered on April 6, 2023, by the Korea Advanced Institute of Science and Technology (KAIST) research team.

Vulnerability	Risk Score	Vendor/ Product	Type of Component/ Software	Malware	Zero-Day
CVE-2023-26083	99	Arm Holdings	GPU Kernel Driver	N/A	Yes
CVE-2023-2033	99	Google	Chrome browser	N/A	Yes
CVE-2023-28205	99	Apple	iPadOS, Safari WebKit, and MacOS Ventura	N/A	Yes
CVE-2023-28206	99	Apple	iPadOS, Safari WebKit, and MacOS Ventura	Pegasus	Yes
CVE-2023-28252	99	Microsoft	Windows servers and clients	Nokoyawa	Yes
CVE-2023-27350	99	PaperCut	PaperCut MF/NG - print management software	Truebot, Clop, LockBit	Yes
CVE-2023-2136	99	Google	Skia (2D graphs library in Google Chrome)	NjRAT	Yes
CVE-2023-29492	95	Novi Systems	Product versions prior to Novi Survey 8.9.43676.	N/A	No

CVE-2023-29199	89	N/A	VM2 Library (JavaScript sandboxing environment)	N/A	No
CVE-2023-30547	89	N/A	VM2 Library (JavaScript sandboxing environment)	N/A	No
CVE-2023-1671	79	Sophos	Sophos Web Appliance	N/A	No
CVE-2023-29017	79	N/A	VM2 Library (JavaScript sandboxing environment)	N/A	No
CVE-2023-29552	79	N/A	Service Location Protocol	N/A	No
CVE-2023-21554	79	Microsoft	Microsoft Message Queuing Service	N/A	No
CVE-2023-28311	77	Microsoft	Microsoft Office	N/A	Yes

Recorded Future®

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.