Recorded Future®

CVE
MONTHLY

Recorded Future CVE Monthly March 2023

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

- Major software vendors disclosed 4 zero-day vulnerabilities in March 2023 that affect both consumer and enterprise products and software, including security features, access control components, and operating systems.
- Microsoft's Windows operating system continues to see new vulnerability exploitation, as befits its high market share.

CVE Monthly Prominent Vulnerability Disclosures

Recorded Future identified 5 newly disclosed vulnerabilities with high risk scores for March 2023, 4 of which are zero-day vulnerabilities, affecting Microsoft, Adobe, Fortinet, and Samsung.

Although we tracked 5 fewer vulnerabilities in March compared to February 2023, 4 of the 5 vulnerabilities identified this month had risk scores of 99 in the Recorded Future Intelligence Cloud, meaning they had a score of "very critical". The number is lower than the 6 very critical vulnerabilities that we tracked in February 2023, but higher than the 2 vulnerabilities ranked with a score of 99 in January.

Microsoft vulnerabilities were once again the most prominent, accounting for 2 of the very critical vulnerabilities: CVE-2023-24880 and CVE-2023-23397. The latter of these vulnerabilities received the most attention this month.

Microsoft released a standalone advisory on March 14, 2023, addressing CVE-2023-23397, a critical vulnerability in Microsoft Outlook that allows an adversary to authenticate as a user to another service using an NTLM relay attack. This is triggered when an attacker sends a message with an extended MAPI property using a universal naming convention (UNC) path to an SMB (TCP 445) share located on a threat actor-controlled server. Microsoft was made aware of the vulnerability following findings from the Computer Emergency Response Team of Ukraine (CERT-UA). Microsoft indicated that it had seen limited, targeted attacks linked to Russian-based threat actors, specifically APT28, targeting organizations in Europe's government, transportation, energy, and military sectors since as early as April 2022. Microsoft also released a script to audit Exchange servers for mail items that might be targets of exploitation.

On March 14, 2023, Google's Threat Analysis Group (TAG) discovered that undisclosed financially motivated threat actors exploited a zero-day Microsoft SmartScreen bypass security vulnerability to deploy the Magniber ransomware. The vulnerability, tracked as CVE-2023-24880, allows an adversary to deliver a malicious Microsoft Software Installer (MSI) file with a specially crafted Authenticode signature that evades Mark of the Web (MOTW) defenses without triggering security warnings.

Analysts identified similar campaigns in which threat actors exploited a Microsoft vulnerability to deploy Magniber ransomware (as well as Qakbot malware). These campaigns occurred in September 2022 and mid-November 2022 and involved the exploitation of a similar Microsoft SmartScreen bypass security vulnerability, tracked as CVE-2022-44698. The difference between the most recent campaigns and the campaigns that occurred in late 2022 is the use of JScript files instead of MSI

files to deliver the Maginiber ransomware payload, as well as the use of a different malformed Authenticode signature to bypass MOTW defenses. Microsoft patched CVE-2022-44698 in December 2022 after the exploitation occurred. Google's TAG identified over 100,000 downloads of the malicious MSI files containing the Magniber ransomware since January 2023. Most users who downloaded the MSI files are from Europe, far from Magniber's usual targets, such as South Korea and Taiwan.

The US Cybersecurity and Infrastructure Agency (CISA) listed CVE-2023-26360 in its Known Exploited Vulnerabilities Catalog on March 15, 2023. CVE-2023-26360 is an improper access control vulnerability affecting Adobe ColdFusion versions before 2021 Update 6 and 2018 Update 16. Threat actors could exploit the vulnerability to execute arbitrary code that takes over the affected device.

On March 7, 2023, Fortinet security researchers released security patches to address a zero-day path traversal vulnerability tracked as CVE-2022-41328. The flaw affects FortiOS and, if exploited, allows a malicious actor to read and write arbitrary files via crafted command-line interface (CLI) commands. The vulnerability affects FortiOS versions 6.4.0 through 6.4.11, 7.0.0 through 7.0.9, 7.2.0 through 7.2.3, and 6.0 and 6.2. Fortinet published a second advisory on March 9, 2023, detailing its investigation of exploitation activity targeting the vulnerability, which also led to its discovery. According to Fortinet, the attacks were conducted by an "advanced actor", and were "highly targeted" against the networks of government organizations.

Fortinet discovered exploitation attempts on March 9, 2023, targeting CVE-2022-41328 when a number of FortiGate and FortiManager devices belonging to one of its customers were targeted and ultimately compromised. At the time of the incident, Fortinet observed sudden, simultaneous system halts and boot failures on all of the affected devices, which displayed the following error message: "FIPS error: Firmware Integrity self-test failed". Fortinet stated that devices enabled with the Federal Information Processing Standards (FIPS) have features that verify the integrity of system components. The error message indicates that an integrity breach was detected, causing the affected device to shut down or encounter boot failures.

In addition to exploitation activity, Fortinet identified the presence of unnamed malware (later identified as VIRTUALPITA, CASTLETAP, VIRTUALPIE, and REPTILE) on the affected devices. On FortiGate devices, activities performed by the malware included exfiltration of data, modification of files, execution of commands via remote shell, and communication with a command-and-control (C2) server. On FortiManager devices, the malware also executed shell commands, exfiltrated files, redirected malicious traffic, modified files, listened to open ports, and disabled firmware on startup.

UNC3886, a China-nexus threat group, is the likely suspect behind a cyber espionage campaign that exploited CVE-2022-41328, according to a March 16, 2023, report by researchers at Mandiant. The goal of these attacks was to establish long-term persistence on and gather intelligence from victim networks. After gaining access, UNC3886 deployed custom malware, such as VIRTUALPITA, CASTLETAP, VIRTUALPIE, and REPTILE for follow-on activities, such as writing files to Fortinet's FortiGate firewall disks while gaining shell access.

The remaining vulnerability listed for this month is CVE-2023-24033, a vulnerability that affects several Samsung Exynos Modem baseband chipsets. A denial of service can result from the format types not being checked specifically by the Session Description Protocol (SDP).

While the mentioned vulnerabilities were discovered in March 2023, there were further developments to vulnerabilities originally tracked and exploited in the past few months. Apple released security

updates on March 27, 2023, to address a zero-day WebKit confusion vulnerability in iPhone and iPad devices, tracked as CVE-2023-23529. The WebKit confusion vulnerability, originally discovered in February, allows a threat actor to execute arbitrary code on compromised devices using specially crafted web content. The affected Apple products are the iPhone 6s, iPhone 7, iPhone SE, iPad Air 2, iPad mini 4, and iPod Touch 7.

Additionally, on March 29, 2023, Google's TAG released an advisory regarding zero-day vulnerabilities in Android, iOS, and Chromium-based browsers (CVE-2022-42856; CVE-2022-4135) that could allow a threat actor to spy on affected devices. In November 2022, threat actors targeted Android and iOS users via SMS phishing messages (Smishing). The majority of victims were in Italy, Malaysia, and Kazakhstan. The SMS contained a URL shortener (bit[.]ly) that redirected the victim to a spoof logistics company or a Malaysian news website. Threat actors exploited iOS vulnerabilities, including CVE-2022-42856, a remote code execution (RCE) vulnerability in WebKit, and CVE-2021-30900, a sandbox escape and privilege escalation vulnerability. The payload delivered to the victim's device allowed a threat actor to install an iOS Application Archive (IPA) file to track a device's location.

In the Android exploit chain, threat actors targeted devices that supported ARM GPU in Google Chrome versions before 106. The exploited vulnerabilities are as follows:

- CVE-2022-4135, which is a heap buffer overflow vulnerability in Chrome GPU
- CVE-2022-3723, which is a type confusion vulnerability in Google Chrome addressed in version 107.0.5304.87
- CVE-2022-38181, which is a privilege escalation vulnerability

Vulnerability	Risk Score	Vendor/ Product	Type of Component/ Software	Malware?	Zero-Day?
CVE-2023-24880	99	Microsoft Windows Server	Security Feature bypass	Magniber	Yes
CVE-2023-23397	99	Microsoft Outlook	Email client		Yes
CVE-2023-26360	99	Adobe ColdFusion	Access Control		Yes
CVE-2022-41328	99	Fortinet	Operating System	VIRTUALPITA, CASTLETAP, VIRTUALPIE, REPTILE	Yes
CVE-2023-24033	79	Samsung	Baseband modem chipsets		No

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.