Recorded Future®

CVE
MONTHLY

Recorded Future CVE Monthly November 2023

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

Key Findings

- In November 2023, 4 zero-day vulnerabilities were identified in products from Microsoft and SysAid IT (an IT service management software), all of which were known to be exploited in the wild.
- The Citrix Bleed vulnerability (CVE-2023-4966) saw increased exploitation in November 2023 — despite being patched in early October — namely by 3 known ransomware groups against multinational corporations.
- Prominent disclosed and exploited vulnerabilities this month affected managed file transfer (MFT) products, Microsoft Windows features (especially SmartScreen), and enterprise IT solutions products such as SysAid IT service management software and VMware's vCloud Director (VCD) appliance.
- Looking ahead, emerging reports indicate that there is a zero-day vulnerability in Google Chrome, CVE-2023-6345, which Google issued a patch for in the face of known exploitation.

In November 2023, we identified 10 high-risk vulnerabilities, 4 of which were zero-day vulnerabilities known to be exploited in the wild. The principal vulnerability trend we observed was the increased exploitation of Citrix Bleed, or CVE-2023-4966, a sensitive information disclosure vulnerability affecting Citrix NetScaler ADC and NetScaler Gateway — we initially reported on this vulnerability in the October 2023 CVE Monthly report. While Citrix Bleed was patched on October 10, 2023, both nation-state and ransomware threat actors exploited Citrix Bleed to carry out attacks throughout October and November 2023. Numerous ransomware groups, including LockBit gang, Medusa gang, and ALPHV, reportedly exploited Citrix Bleed to attack enterprises, including ICBC (which was confirmed by the US Treasury), DP World, Allen & Overy, Toyota Financial Services (TFS), and Fidelity National Inc this month [1, 2, 3].

These events echo similar patterns of mass exploitation of vulnerabilities by CL0P ransomware group (CL0P), most notably its widespread exploitation of a vulnerability in MOVEit Transfer managed file transfer (MFT) service between late May 2023 and mid-August 2023. In another parallel to CL0P exploits this month, threat actors targeted a vulnerability (CVE-2023-49103) in another MFT service, ownCloud. CVE-2023-49103 can enable threat actors to steal ownCloud administrative passwords, mail server credentials, license keys, and server configuration information. CVE-2023-49103 was disclosed on November 21, 2023, and threat researchers observed the active exploitation of CVE-2023-49103 starting on November 25, 2023. CrushFTP, yet another file transfer product, had a high-risk unauthenticated remote code execution (RCE) vulnerability disclosed this month; on November 16, 2023, Converge Technology Solutions (Converge) publicly disclosed detailed proof of concept (PoC) exploit code for CVE-2023-49103, increasing its chances of being actively exploited.

In exploitation affecting major software vendors, Microsoft and the US Cybersecurity Infrastructure Security Agency (CISA) issued exploitation warnings for 3 vulnerabilities affecting Windows features: Microsoft Windows SmartScreen, Microsoft Windows Desktop Window Manager (DWM) Core Library, and Microsoft Windows Cloud Files Mini Filter Driver. We assess that of the 3, Windows SmartScreen has the highest demand from threat actors for exploitation based on 2 factors preceding and following the vulnerability's announcement. First, we identified discussion on online forums surrounding disabling SmartScreen prior to mid-November, indicating interest in the product.

Following the advisories in mid-November, media reports stated that the APT group known as TA544 was known to have exploited CVE-2023-36025 using Remcos RAT.

There were 2 vulnerabilities affecting enterprise IT solutions this month. A zero-day vulnerability in SysAid IT service management software, tracked as CVE-2023-47246, was known to have been exploited in the wild, particularly by Lace Tempest, a threat actor that distributes CL0P ransomware. Second, CVE-2023-34060 in VMware's vCloud Director (VCD) appliance allows threat actors to bypass login restrictions on specific ports to access target networks.

For the remainder of 2023, emerging reports indicate that there is an exploited zero-day vulnerability in Google Chrome: CVE-2023-6345, which is an integer overflow flaw affecting the open-source 2D graphics engine known as Skia. This echoes a number of zero-days in Google Chrome that emerged in December 2022 (with 2 vulnerabilities announced within just 8 days of each other), which made for a busy end-of-year for Chrome defenders (1, 2). Below, we further discuss the top vulnerabilities disclosed in November 2023:

CVE-2023-49103 (ownCloud) Can Enable Theft of ownCloud Administrative Credentials and More

A newly disclosed vulnerability (CVE-2023-49103, CVSSv3.1 Score: 10), which affects the ownCloud managed file transfer (MFT) service, can enable threat actors to steal ownCloud administrative passwords, mail server credentials, license keys, and server configuration information. Proof-of-concept exploit code was published for the vulnerability on GitHub on November 22, 2023.

CVE-2023-43177 (CrushFTP) Can Enable an Unauthenticated Attacker to Hijack Accounts, Escalate Privileges, and Compromise CrushFTP Instances

A CrushFTP remote code execution (RCE) vulnerability (CVE-2023-43177) can enable an unauthenticated attacker to hijack accounts, escalate privileges, and compromise CrushFTP instances. The vulnerability was initially discovered and reported by Converge Technology Solutions (Converge) on August 8, 2023, and swiftly patched by the CrushFTP development team on August 9, 2023. In an updated advisory published on November 16, 2023, CrushFTP classified the vulnerability as "severe" and urged customers to remediate the vulnerability immediately if they had not already done so.

3 Microsoft Vulnerabilities Being Actively Exploited in the Wild

On November 14, 2023, the US Cybersecurity Infrastructure Security Agency (CISA) added 3 Microsoft vulnerabilities to its Known Exploited Vulnerability (KEV) catalog based on evidence of active exploitation. This is in line with Microsoft's publication of its Patch Tuesday report, which issued patches for these and other flaws. The 3 vulnerabilities are:

- CVE-2023-36025 — a security feature bypass vulnerability in Microsoft Windows SmartScreen that can be exploited to deliver malicious content
- CVE-2023-36033 — a privilege escalation vulnerability in Microsoft Windows Desktop Window Manager (DWM) Core Library that can be exploited to gain SYSTEM privileges
- CVE-2023-36036 — a privilege escalation vulnerability in Microsoft Windows Cloud Files Mini Filter Driver that can be exploited to gain SYSTEM privileges

While CISA stated that the vulnerabilities had been exploited, CISA did not provide more details on threat actors, victims, or other TTPs associated with exploitation; CISA's vulnerability advisories seldom expand on the exploitation activity itself. As with all vulnerabilities added to the KEV, US

federal civilian agencies are mandated to remediate them across their infrastructure within a certain period of time (in this case, by December 5, 2023).

Zero-Day Vulnerability in SysAid IT Exploited by Lace Tempest
Microsoft's threat intelligence team has observed that a zero-day vulnerability in SysAid IT service management software, tracked as CVE-2023-47246, has been exploited in the wild, the team reported on November 8, 2023. The vulnerability was exploited by Lace Tempest, a threat actor who distributes CL0P ransomware. Microsoft notified SysAid about the vulnerability, which it immediately patched.

SysAid confirmed that its SysAid on-premises software is affected by the vulnerability, which it described as a path traversal issue leading to arbitrary code execution. SysAid also shared technical information on the observed attack including indicators of compromise (IoCs) as well as recommendations.

VMware Discloses Cloud Director Appliance Authentication Bypass Vulnerability, CVE-2023-34060
On November 14, 2023, VMware disclosed a critical authentication bypass vulnerability in its vCloud Director (VCD) appliance, tracked as CVE-2023-34060. CVE-2023-34060 allows unauthenticated threat actors with network access to bypass login restrictions when authenticating on specific ports. The vulnerability affects deployments of VCD Appliance 10.5 that were upgraded from older releases. The bypass is not present on a new installation of VCD Appliance 10.5. The upgraded and patched version of VCD Appliance can be found here.

QNAP Patches Vulnerability Operating System and Application Versions

On November 4, 2023, QNAP disclosed and patched a critical OS command injection vulnerability (CVE-2023-23369) affecting certain versions of QNAP operating systems and applications, including its multimedia console and media streaming add-on. The vendor did not state that the vulnerability was known to be exploited in the wild in its disclosures.

Google Patches Actively Exploited Chrome Zero-Day Flaw, CVE-2023-6345
Google patched an actively exploited vulnerability tracked as CVE-2023-6345, which is an integer overflow flaw affecting Skia, an open-source 2D graphics engine, on November 28, 2023. Skia resides in Google products such as Google Chrome and ChromeOS, among others. While Google acknowledged that threat actors are actively exploiting CVE-2023-6345 in the wild, it did not provide additional details.

CVE Monthly Prominent Vulnerability Disclosures

In the table below, actively exploited vulnerabilities affecting the 8 major software vendors are highlighted in gray.

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/ Component	Zero-Day
1	CVE-2023-36025	99	Microsoft Windows SmartScreen	Security feature bypass vulnerability affecting Windows SmartScreen	Yes
2	CVE-2023-36033	99	Microsoft Windows Desktop Window Manager (DWM) Core Library	Privilege escalation vulnerability affecting DWM Core Library	Yes
3	CVE-2023-36036	99	Microsoft Windows Cloud Files Mini Filter Driver	Privilege escalation vulnerability affecting filter driver	Yes
4	CVE-2023-47246	99	SysAid IT On-Premise software	Directory traversal vulnerability affecting on-premise software	Yes
5	CVE-2023-49103	79	ownCloud managed file transfer (MFT) service	Information disclosure vulnerability affecting the Graph API application component	No
6	CVE-2023-43177	79	CrushFTP	Remote code execution (RCE) vulnerability affecting protocol headers within CrushFTP	No
7	CVE-2023-48365	79	Qlik Sense	An unauthenticated remote code execution vulnerability affecting Qlik Sense Enterprise for Windows before the August 2023 Patch	No
8	CVE-2023-23368	77	QNAP operating system	An OS command injection vulnerability has been reported to affect several QNAP operating system versions	No
9	CVE-2023-34060	77	VMware vCloud Director (VCD) appliance	Authentication bypass vulnerability affecting VCD appliance	No
10	CVE-2023-23369	75	QNAP operating system	OS command injection vulnerability affecting operating systems, multimedia consoles, and media streaming add-on	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 threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence. Learn more at recordedfuture.com.