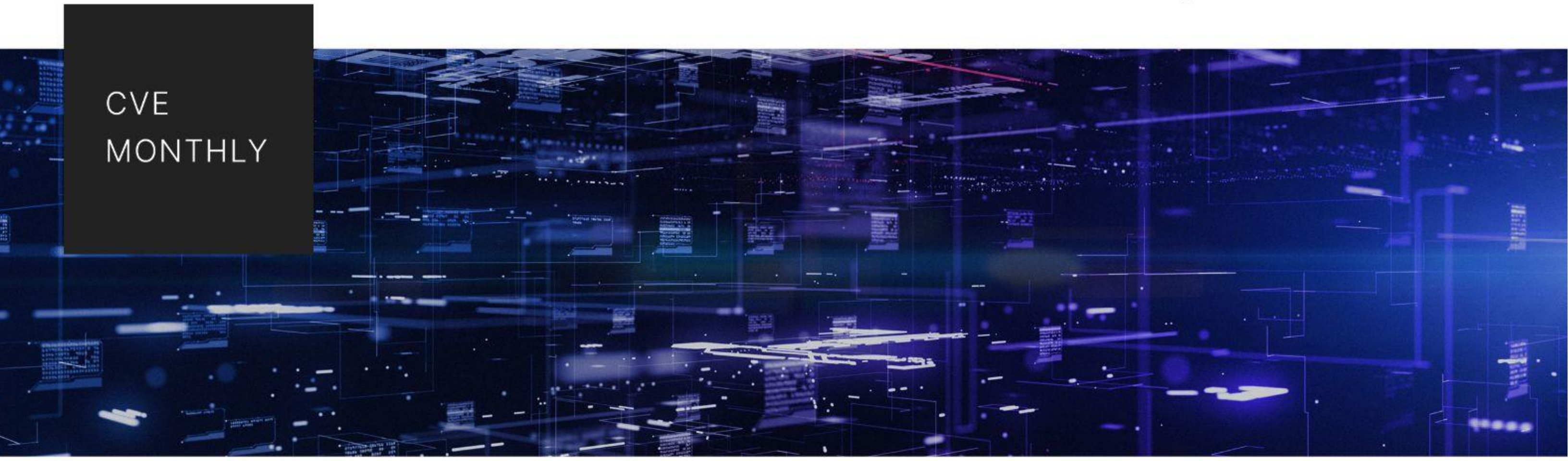
Recorded Future®



Recorded Future CVE Monthly July 2023

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

- In July 2023, 10 confirmed zero-day vulnerabilities affected Microsoft, Adobe, Apple, and Ivanti products.
- Microsoft patched 5 zero-day vulnerabilities in July 2023.
- CL0P Ransomware Group continued to exploit vulnerabilities in Progress Software's MOVEit Transfer managed file transfer (MFT), bringing the total number of MOVEit attack victims to more than 500 as of July 31, 2023.
- Apple patched a fourth zero-day vulnerability exploited in Operation Triangulation, which reportedly targeted Russian nationals starting in 2019.
- 28 of the approximately 2,300 vulnerabilities disclosed in July 2023 were high-risk, according to Recorded Future data.

CVE Monthly Prominent Vulnerability Disclosures

We identified 28 newly disclosed vulnerabilities with high risk scores for July 2023, 10 of which are zero-day vulnerabilities affecting Microsoft, Apple, Adobe, and Ivanti products. The 3 zero-day vulnerabilities that attracted some of the highest attention according to our data set were all exploited in high-profile threat campaigns that targeted government entities. A Microsoft and an Apple vulnerability were each exploited by different threat actors to enable 2 separate cyber-espionage campaigns. CVE-2023-36884 is a remote code execution vulnerability in Microsoft Office and Windows HTML, exploitation of which has been attributed to the threat actor known as Storm-0978. CVE-2023-38606 is a kernel flaw affecting devices that use iOS, iPadOS, and macOS and is the fourth Apple zero-day vulnerability that has been connected to Operation Triangulation, according to Kaspersky researchers. CVE-2023-35078, the third zero-day vulnerability exploited in a high-profile campaign to target government entities, is an unauthenticated access vulnerability in the Ivanti Endpoint Manager Mobile (EPMM) application that allows remote, internet-facing threat actors to obtain unauthenticated access to the EPMM API endpoint; threat actors exploited CVE-2023-35078 to compromise 12 unnamed Norwegian ministries.

By confirmed victim counts, the most widely exploited vulnerabilities in July 2023 affected Progress Software's MOVEit Transfer. Progress Software patched 3 additional MOVEit Transfer vulnerabilities in July 2023. It is unclear at this time which specific MOVEit vulnerabilities CL0P Ransomware Group (CL0P) is exploiting to carry out its attacks. Additional MOVEit Transfer attacks have brought the total victim count to more than 500 as of July 31, 2023. Details of MOVEit Transfer vulnerabilities and their exploitation were also featured in our May 2023 and June 2023 CVE rollup reports.

Further details about the zero-day vulnerabilities that were disclosed this month are highlighted below. We also provide an update on the continued exploitation of vulnerabilities in Progress Software's MOVEit Transfer MFT service by CL0P Ransomware Group, and detail 2 Rockwell Automation industrial control system (ICS) vulnerabilities that were connected to the exploitation capabilities of an unnamed threat actor (although neither vulnerability was confirmed to be exploited in the wild).

Widespread Attacks Continue to Target Progress Software MOVEit Transfer

CL0P Ransomware Group continued to conduct widespread attacks on vulnerable instances of Progress Software's MOVEit Transfer MFT service in July 2023. Between July 25 and 26, 2023, alone, Recorded Future data shows that CL0P posted over 60 likely MOVEit victims to its dark web extortion site. As of July 31, 2023, over 500 organizations have been affected by attacks on MOVEit Transfer. In each case, the specific MOVEit Transfer vulnerabilities exploited to carry out the attacks are not confirmed. Details on 3 additional MOVEit Transfer vulnerabilities patched in July 2023 are available here.

Microsoft Addressed More Than 130 Vulnerabilities in July 2023; 5 Exploited in the Wild

On July 11, 2023, Microsoft addressed more than 130 vulnerabilities in its July 2023 Patch Tuesday. 9 were classified as critical, and 5 of those 9 were actively exploited zero-day vulnerabilities. The vulnerabilities are found in various Microsoft products, drivers, and software, and are detailed below.

CVE-2023-36884, a remote code execution vulnerability in Microsoft Office and Windows HTML, should be prioritized for patching as it is associated with a Storm-0978 (known for deploying the RomCom RAT malware) threat campaign that targeted "defense and government entities in Europe and North America". In this campaign, an adversary can deploy a specially crafted Microsoft Office document to lure victims into executing a malicious file that leads to remote code execution.

CVE-2023-36874 and CVE-2023-32046 are both elevation-of-privilege vulnerabilities in the Windows Error Reporting Service and the MSHTML Platform. Both vulnerabilities were exploited in the wild. To exploit CVE-2023-36874, an adversary must have local access to the target system and have certain user privileges. To exploit CVE-2023-32046, an adversary creates a specially crafted malicious file and lures the victim to access it via social engineering techniques. Both of the vulnerabilities allow the adversary to gain administrator privileges.

CVE-2023-32049 and CVE-2023-35311 are security feature bypass vulnerabilities in Windows SmartScreen and Microsoft Outlook. Both vulnerabilities can be exploited by an adversary by luring their victims into accessing a specially crafted URL that bypasses security detections. Notably, CVE-2023-32049 is similar to other Mark of the Web (MOTW) vulnerabilities in which the adversaries can deploy a malicious file that bypasses MOTW defenses.

2 Adobe ColdFusion Vulnerabilities Exploited to Install Webshells

On July 17, 2023, Rapid7 reported that 2 vulnerabilities in Adobe ColdFusion, CVE-2023-29298 and CVE-2023-38203, were exploited in the wild. CVE-2023-29298 is an initial access bypass vulnerability. By exploiting this vulnerability, threat actors can circumvent access restrictions and gain unauthorized access to sensitive information or perform unauthorized actions on the affected system. This can include stealing data, manipulating data, or injecting malicious code into legitimate applications. CVE-2023-38203 is a critical remote code execution vulnerability that allows unauthenticated visitors to execute commands on vulnerable ColdFusion 2018, 2021, and 2023 servers.

According to Rapid 7, attackers chained CVE-2023-29298 and CVE-2023-38203 together to execute PowerShell commands to create a webshell. Webshells are malicious scripts or programs that provide persistent access to and remote control of a compromised system. Once they are installed, threat actors can use the webshells to maintain remote access, execute commands, steal data, or move laterally to other systems within the network.

This is the second incident in recent months involving in-the-wild exploitation of a vulnerability affecting Adobe ColdFusion. On March 15, 2023, the US Cybersecurity and Infrastructure Agency (CISA) listed CVE-2023-26360 in their Known Exploited Vulnerabilities (KEV) Catalog. 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. Adobe was aware of CVE-2023-26360 being exploited by threat actors in limited attacks against Adobe ColdFusion.

Defenders using Adobe ColdFusion versions 2018, 2021, and 2023 should consult Adobe's security bulletin that provides updates to address CVE-2023-29298 and CVE-2023-38203. Adobe also recommends applying the security configuration settings documented on the ColdFusion Security page.

Apple Released Emergency Update for Zero-Day Vulnerability CVE-2023-37450

On July 10, 2023, Apple released Rapid Security Response (RSR) updates for macOS, iOS, and iPadOS to address a new zero-day vulnerability, CVE-2023-37450, in the WebKit browser engine. CVE-2023-37450, which was reported by an anonymous security researcher, can enable arbitrary code execution on targeted devices if targets are lured to open malicious web pages. RSR patches were recently introduced by Apple to quickly mitigate zero-day vulnerabilities in macOS, iOS, and iPadOS between regularly scheduled software updates.

There are no specific details providing insight into how CVE-2023-37450 has been exploited in real-life scenarios. Apple does not typically disclose technical details about zero-day vulnerabilities, in order to slow threat actors' ability to develop and deploy new exploits that target vulnerable devices. This was the tenth zero-day vulnerability that Apple has patched in 2023; the eleventh, CVE-2023-38606, is detailed below.

Apple Patched Fourth Zero-Day Vulnerability Reportedly Exploited in Operation Triangulation

In late July 2023, Apple patched another zero-day vulnerability (CVE-2023-38606) that, according to Kaspersky researcher Boris Larin, was exploited to carry out Operation Triangulation; this is the fourth Apple vulnerability that has been linked to Operation Triangulation, a spyware campaign that reportedly targeted Russian nationals starting in 2019.

On July 24, 2023, Apple released a patch for CVE-2023-38606, a kernel flaw affecting devices that use iOS, iPadOS, and macOS, and credited the following Kaspersky researchers with its discovery: Valentin Pashkov, Mikhail Vinogradov, Georgy Kucherin, Leonid Bezvershenko, and Boris Larin. Apple disclosed that the flaw could be used to "modify sensitive kernel state", but otherwise did not release details about how the flaw allows kernel modification. According to Boris Larin, CVE-2023-38606 was another vulnerability that was exploited in service of Operation Triangulation.

Kaspersky researchers previously linked Operation Triangulation to 3 other recently patched Apple vulnerabilities. CVE-2023-32434 allows an application with kernel privileges to perform code execution when exploited. CVE-2023-32435 and CVE-2023-32439 are Apple WebKit vulnerabilities that lead to code execution when executing maliciously crafted web content. The vulnerabilities also affect a wide range of Apple products that use iOS, iPadOS, macOS, watchOS, and Safari WebKit. Apple released patches for all 3 zero-day vulnerabilities on June 21, 2023.

The details of Operation Triangulation were publicized by the Moscow-based cybersecurity company Kaspersky in June 2023, after the malware was detected on iPhones within its network. Operation Triangulation operators attack their targets by sending iMessages with malicious attachments.

Kaspersky stated that an implant was deployed on a targeted device after operators exploited an unspecified kernel vulnerability. The Russian government previously blamed Operation Triangulation on the US; however, there is no additional evidence from open sources to confirm that these accusations are true. The threat actor behind Operation Triangulation is not known at this time.

Ivanti Patched Zero-Day Vulnerability CVE-2023-35078 in Endpoint Manager Mobile (EPMM) Product

On July 24, 2023, Ivanti Software Inc. patched a zero-day authentication bypass vulnerability in its Endpoint Manager Mobile (EPMM) product, formerly called MobileIron Core. EPMM is a mobile device management (MDM) platform. The vulnerability, tracked as CVE-2023-35078, allows remote, internet-facing attackers to obtain unauthenticated access to the EPMM API endpoint. According to an alert by the US Cybersecurity and Infrastructure Security Agency (CISA) on July 24, 2023, attackers can use API access to view EPMM users' personally identifiable information (PII) such as names, phone numbers, emails, and passwords. CISA said that CVE-2023-35078 also allows threat actors to make configuration changes to EPMM servers, including adding an administrative account to escalate privileges. Ivanti itself did not confirm exploitation of CVE-2023-35078 in the wild; however, the company's advisory states that a "credible source" observed exploitation of CVE-2023-35078 in a "limited number" of attacks.

Despite Invanti not linking the vulnerability to any attacks specifically, on July 24, 2023, the Norwegian National Security Authority and the Departments' Security and Service Organization (DSS) announced that threat actors exploited CVE-2023-35078 to compromise 12 unnamed Norwegian ministries. DSS stated that the vulnerability has not affected Norway's government operations, and that it is "investigating and handling the incident with assistance from the National Security Authority (NSM)". According to the DSS, the breach did not affect the Prime Minister's office, the Norwegian Ministry of Defence, the Norwegian Ministry of Justice and Emergency Preparedness, and the Norwegian Ministry of Foreign Affairs, as they do not use the EPMM platform. DSS did not attribute the cyberattacks to a specific threat actor.

The vulnerability affects EPMM versions 11.10, 11.9, and 11.8, as well as older end-of-life installations. Ivanti released security patches for CVE-2023-35078 on July 23, 2023, and advised all users to upgrade to EPMM versions 11.8.1.1, 11.9.1.1, and 11.10.0.2. Ivanti stated that it has not found evidence that there was a supply-chain attack or that the vulnerability affects the company's code development process.

2 Rockwell Automation Vulnerabilities Were Tied to the Exploit Capabilities of an Unspecified APT Group

2 newly disclosed vulnerabilities that affect Rockwell Automation products have been tied to the exploit capabilities of an unspecified advanced persistent threat (APT) group, according to a July 12, 2023, Dragos report. The vulnerabilities, CVE-2023-3595 and CVE-2023-3596, affect Rockwell Automation's ControlLogix EtherNet/IP (ENIP) communication modules. Rockwell Automation products are commonly used in manufacturing, electric, oil, water, and transportation and gas industries and sectors.

While confirming that the unnamed APT had access to the vulnerabilities, Dragos reported that there was "no evidence of exploitation in the wild". Dragos also noted that such forewarning of an APT-owned vulnerability prior to exploitation is rare, offering a critical opportunity to proactively defend critical infrastructure.

#	Vulnerability	Risk Score	Affected Vendor/ Product	Type of Component/ Software	Malware	Zero-Day
1	CVE-2023-32046	99	Microsoft Windows (10, 11, Server)	Operating System	N/A	Yes
2	CVE-2023-32049	99	Windows SmartScreen, Microsoft Outlook	Software Application	N/A	Yes
3	CVE-2023-36874	99	Windows Error Reporting Service, MSHTML Platform	Software Application	N/A	Yes
4	CVE-2023-35311	99	Windows SmartScreen, Microsoft Outlook	Software Application	N/A	Yes
5	CVE-2023-36884	89	Microsoft Office, Windows HTML	Software Application	N/A	Yes
6	CVE-2023-36934	99	Progress Software MOVEit Transfer MFT	Software Application	N/A	Possibly
7	CVE-2023-29300	99	Adobe ColdFusion	Software Application	N/A	Possibly
8	CVE-2023-29298	99	Adobe ColdFusion	Software Application	N/A	Yes
9	CVE-2023-38203	99	Adobe ColdFusion	Software Application	N/A	Yes
10	CVE-2023-35078	99	Ivanti Endpoint Manager Mobile	Software Application	N/A	Yes
11	CVE-2023-38606	99	macOS, iOS, iPadOS	Kernel	N/A	Yes
12	CVE-2023-37450	99	macOS, iOS, iPadOS	Apple WebKit Browser Engine	N/A	Yes
13	CVE-2023-26258	89	Arcserve Unified Data Protection (UDP)	Software Application	N/A	No
14	CVE-2023-30799	79	MikroTik RouterOS	Operating System	N/A	No
15	CVE-2023-35086	79	ASUS Router	Router	N/A	No

#	Vulnerability	Risk Score	Affected Vendor/ Product	Type of Component/ Software	Malware	Zero-Day
16	CVE-2023-3595	79	Rockwell Automation's ControlLogix EtherNet/IP (ENIP)	Communication Modules	N/A	No
17	CVE-2023-3596	79	Rockwell Automation's ControlLogix EtherNet/IP (ENIP)	Communication Modules	N/A	No
18	CVE-2023-24489	79	Citrix ShareFile Storage Zones Controller	Software Application	N/A	No
19	CVE-2023-38408	79	OpenSSH's Forwarded ssh-agent background program	Background Program	N/A	No
20	CVE-2023-34329	79	Ami MegaRAC SP-X	Software/Firmware Server Management Solution	N/A	No
21	CVE-2023-34330	79	Ami MegaRAC SP-X	Software/Firmware Server Management Solution	N/A	No
22	CVE-2023-34192	79	Zimbra Collaboration Suite	Software Application	N/A	No
23	CVE-2022-24834	79	Redis (database management system)	Open-Source In-Memory Storage System	N/A	No
24	CVE-2023-37582	79	Apache RocketMQ	Software Application	N/A	No
25	CVE-2023-33148	79	Microsoft Office	Software Application	N/A	No
26	CVE-2023-36460	78	Joinmastodon Mastodon	Open-Source Social Network Platform	N/A	No
27	CVE-2023-21250	76	Google Android OS	Operating System	N/A	No
28	CVE-2023-22814	75	Western Digital My Cloud OS	Operating System	N/A	No

Note: Actively exploited vulnerabilities affecting the 8 major software vendors are highlighted in gray.

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.