Recorded Future®

CVE
MONTHLY

Recorded Future CVE Monthly June 2023

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

- 8 zero-day vulnerabilities in June 2023 affected Progress Software, VMware, Apple, Fortinet, and Zyxa products.
- Vulnerabilities in Progress Software's MOVEit Transfer file transfer solution were exploited to carry out attacks on approximately 75 organizations across public and private sectors.
- Vulnerabilities in Apple products were implicated in the threat campaign, known as Operation Triangulation, which reportedly targeted Russian nationals.
- 18 of the approximately 2,200 vulnerabilities disclosed in June 2023 were high-risk.
- Microsoft did not disclose or patch any confirmed zero-day vulnerabilities in June 2023.

CVE Monthly Prominent Vulnerability Disclosures

We identified 18 newly disclosed vulnerabilities with high risk scores for June 2023, 8 of which are zero-day vulnerabilities affecting Progress Software, VMware, Apple, Fortinet, and Zyxel products. The 3 zero-day vulnerabilities that attracted some of the highest attention from security researchers according to our data set were CVE-2023-34362, a SQL injection vulnerability in Progress Software's MOVEit Transfer file transfer solution (also featured in last month's report); CVE-2023-20887, a critical command injection vulnerability affecting VMware Aria Operations for Network; and CVE-2023-32434, an integer overflow vulnerability (affecting a wide range of Apple products) that when exploited, can enable an application with kernel privileges to perform malicious code execution.

CVE-2023-32434 was reportedly instrumental in Operation Triangulation, a spyware campaign that targeted Russian nationals starting in 2019. CVE-2023-34362 was also featured in the CVE monthly report for May 2023; however, since its initial disclosure on May 31, 2023, it has become the most prominent June 2023 vulnerability based on the number of victims its exploitation has affected. Throughout June 2023, vulnerabilities in MOVEit Transfer have been exploited to enable high-profile attacks on approximately 70 organizations across the public and private sectors.

In a departure from previous months, Microsoft did not disclose or patch any zero-day vulnerabilities in June 2023.

Progress Software's MOVEit Transfer (CVE-2023-34362)
After its initial disclosure on May 31, 2023, CVE-2023-34362 was widely exploited by threat actors to carry out successful cyberattacks throughout June 2023. Reports indicated that attacks involving the exploitation of CVE-2023-34362 targeting MOVEit Transfer instances started at least as early as May 27, 2023. On June 4, 2023, Microsoft linked widespread exploitation of CVE-2023-34362 to CL0P Ransomware Group (Clop).

Cybersecurity and Infrastructure Security Agency (CISA) officials told reporters on June 15, 2023, that hundreds of US companies and organizations could be affected by attacks targeting MOVEit Transfer. CISA Director Jen Easterly disclosed that an unspecified number of federal agencies were affected by vulnerabilities in their MOVEit Transfer instances and that federal authorities were assessing the scope of potential intrusions into federal government-used instances of MOVEit Transfer, as well as the risks faced by all federal agencies that use the application. Easterly

downplayed the severity of the incidents, noting that "this is not a campaign like SolarWinds that presents a systemic risk to our national security or our nation's network".

As of June 30, 2023, at least 75 organizations have been confirmed to be affected by the exploitation of vulnerable MOVEit Transfer applications. Attacks have resulted in high-profile data exposure incidents across the public and private sectors. Notable victims have so far included the US Department of Energy, the Louisiana Office of Motor Vehicles, Gen Digital (cybersecurity company that owns Norton, Avast, LifeLock, Avira, AVG, ReputationDefender, and CCleaner), Shell, BBC, British Airways, Schneider Electric, and Siemens Energy, among others.

In June 2023, Progress Software disclosed, patched, and provided remediation instructions for 2 additional vulnerabilities in MOVEit Transfer: CVE-2023-35036 (disclosed on June 9, 2023); and CVE-2023-35708 (disclosed on June 15, 2023). Attacks are likely to continue on vulnerable instances of Progress Software's MOVEit Transfer MFT service. If they have not done so already, organizations are urged to view Progress Software's advisories [1, 2, 3] for CVE-2023-34362, CVE-2023-35036, and CVE-2023-35708, and follow instructions for both hardening and patching MOVEit Transfer MFT instances. On June 7, 2023, Mandiant published a guide to both containing and hardening systems against attacks via CVE-2023-34362. Additionally, on June 7, 2023, CISA published an advisory addressing the recent exploitation of CVE-2023-34362.

The exploitation of vulnerabilities in file transfer services has recently become a popular way by which threat actors, especially those affiliated with Clop, gain access to sensitive data on corporate networks. The widespread exploitation of CVE-2023-34362 has parallels to a vulnerability in another file transfer service, Fortra's GoAnywhere managed file transfer (MFT). Despite being patched since February 2023, Clop and other threat groups were able to repeatedly exploit CVE-2023-0669, a GoAnywhere MFT vulnerability, to carry out successful, high-profile cyberattacks up to at least May 2023.

VMware Aria Operations (CVE-2023-20887)

On June 20, 2023, VMware confirmed that CVE-2023-20887 had been exploited in the wild. Researchers at GreyNoise initially reported CVE-2023-20887 on June 7, 2023. The vulnerability is exploitable when a vulnerable vRealize Network Insight accepts user input in the Apache Thrift RPC Interface. The vulnerability could be abused to execute arbitrary commands in the context of the root user. On June 15, 2023, SinSinology researchers released a POC exploit code for CVE-2023-20887. The POC exploit highlighted how unauthenticated threat actors could abuse the vulnerability to achieve remote code execution (RCE). Furthermore, GreyNoise provided a "dedicated tag" that allows organizations to track IP addresses that attempt to exploit CVE-2023-20887. Users of VMware should download the patch build number 1685358321 to address the vulnerability.

VMware addressed 2 other vulnerabilities in Aria Operations this month: CVE-2023-20888 (authenticated deserialization vulnerability) and CVE-2023-20889 (information disclosure vulnerability). Neither was confirmed to have been exploited in the wild, as of this writing.

Apple Products (CVE-2023-32434, CVE-2023-32435, CVE-2023-32439)
On June 1, 2023, Apple released patches for 2 zero-day vulnerabilities (CVE-2023-32434 and CVE-2023-32439) reportedly exploited in a spyware campaign dubbed Operation Triangulation, which the Russian government previously blamed on the US. CVE-2023-32434 and CVE-2023-32439 were each reported to Apple by Kaspersky researchers. The details of Operation Triangulation were publicized [1, 2] by the Moscow-based cybersecurity company Kaspersky in June 2023, after the malware was detected on iPhones within its network. Operation Triangulation has reportedly been active since 2019; its operators attack its targets by sending iMessages with malicious attachments. CVE-2023-32439 is an Apple WebKit vulnerability that, if exploited, can enable the execution of maliciously crafted web content. Neither bug is known to have affected devices newer than iOS 15.7.

On June 23, 2023, CISA added CVE-2023-32434 and CVE-2023-32439, along with CVE-2023-32435 (also an Apple WebKit vulnerability that can enable the execution of maliciously crafted web content), to its Known Exploited Vulnerabilities Catalog (KEV).

Fortinet FortiOS and FortiProxy SSL-VPNs (CVE-2023-27997)
On June 12, 2023, Fortinet published an advisory and write-up for the critical heap-based buffer overflow vulnerability tracked as CVE-2023-27997 (FG-IR-22-398) that allows remote code execution (RCE) in vulnerable FortiOS and FortiProxy SSL-VPNs instances. According to the accompanying blog write-up, Fortinet observed a limited number of cases of exploitation in the wild.

The vulnerability was initially discovered and reported to Fortinet by security researchers Charles Fol and Dany Bach from LEXFO. Fol stated to BleepingComputer that this "should be considered an urgent patch" for Fortinet administrators. In a blog post, the researchers stated that the bug resides in the web interface that authenticates to the VPN. Threat actors can control both the size of the allocated buffer and the amount of overflow, allowing them to cause an artificial overflow of information and be able to execute custom logic.

Fortinet's advisory was published a few days after a patch for the vulnerability was disseminated to Fortinet customers, which occurred as early as June 9, 2023. Fortinet often issues patches before announcing the vulnerability publicly, to prevent widespread reverse-engineering of patches by threat actors.

Zyxel NAS Firmware (CVE-2023-27992)
On June 20, 2023, Zyxel warned its users that firmware in its NAS (Network Attached Storage) device were affected by a critical pre-authentication command injection vulnerability (CVE-2023-27992) that could allow an unauthenticated user to execute operating system commands by sending specially crafted HTTP requests. Zyxel instructed users to update their NAS firmware immediately. On June 23, 2023, CISA added CVE-2023-27992 to its KEV Catalog.

Microsoft Exchange Server and SharePoint Server (CVE-2023-32031, CVE-2023-29357)
Microsoft patched 78 vulnerabilities, including 38 remote code execution (RCE) vulnerabilities, as part of its June 2023 Patch Tuesday. None of the vulnerabilities were zero-days, nor have any been confirmed to be exploited in the wild, as of this writing. Of the 78, 2 high-risk vulnerabilities, per Recorded Future data, includes CVE-2023-32031, an RCE vulnerability in Microsoft Exchange Server, and CVE-2023-29357, an elevation of privilege vulnerability in Microsoft SharePoint Server.

Cisco AnyConnect Secure Mobility Client Software and Cisco TelePresence Video Communication Server (CVE-2023-20178, CVE-2023-20105)

PoC exploit code for CVE-2023-20178, a high-risk privilege escalation vulnerability in Cisco AnyConnect Secure Mobility Client Software for Windows and Cisco Secure Client Software for Windows, was published by security researcher Filip Dragović. Dragović also initially reported on the vulnerability. The exploit was tested against Cisco Secure Client (tested on 5.0.01242) and Cisco AnyConnect (tested on 4.10.06079). Defenders can access the update in Cisco's advisory for more information.

On June 7, 2023, Cisco reported CVE-2023-20105, a vulnerability in Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) that could allow an "authenticated attacker with Administrator-level read-only credentials to elevate their privileges to Administrator with read-write credentials on an affected system".

As of this writing, neither CVE-2023-20178 nor CVE-2023-20105 are confirmed to have been exploited in the wild. This continues a trend of Cisco reporting and patching vulnerabilities with high criticality ratings that have not been not been confirmed to be actively exploited.

#	Vulnerability	Risk Score	Vendor/ Product	Type of Component/ Software	Malware	Zero-Day
1	CVE-2023-20887	99	VMware Aria Operations	Network Management Software	N/A	Yes
2	CVE-2023-34362	99	Progress Software MOVEit Transfer	MFT Software	Clop Ransomware	Yes
3	CVE-2023-32434	99	Apple, Multiple OSs	Operating System	Operation Triangulation Malware	Yes
4	CVE-2023-32435	99	Apple Safari	Browser	Operation Triangulation Malware	Yes
5	CVE-2023-32439	99	Apple Safari	Browser	N/A	Yes
6	CVE-2023-27992	99	Zyxel NAS	Cloud Storage Firmware	N/A	Yes
7	CVE-2023-27997	99	Fortinet FortiOS and FortiProxy SSL-VPNs	Multiple	Unspecified Ransomware	Yes
8	CVE-2023-20105	82	Cisco TelePresence Video Communication Server (VCS) and Expressway Series	Multiple	N/A	No

#	Vulnerability	Risk Score	Vendor/ Product	Type of Component/ Software	Malware	Zero-Day
9	CVE-2023-32031	79	Microsoft Exchange Server	Server	N/A	No
10	CVE-2023-20888	79	VMware Aria Operations	Network Management Software	N/A	Yes
11	CVE-2023-35036	79	Progress Software MOVEit Transfer	MFT Software	N/A	Possibly
12	CVE-2023-35708	79	Progress Software MOVEit Transfer	MFT Software	N/A	Possibly
13	CVE-2023-33965	79	Txthinking Brook	Cross-Platform Programmable Network Tool	N/A	No
14	CVE-2023-33733	79	ReportLab PDF Toolkit	Open-Source Engine	N/A	No
15	CVE-2023-20178	79	Cisco AnyConnect Secure Mobility Client	Windows Software	N/A	No
16	CVE-2023-33476	79	Readymedia Project	Server Software	N/A	No
17	CVE-2023-0667	75	Wireshark	Open-Source Packet Analyzer	N/A	No
18	CVE-2023-29357	75	Microsoft SharePoint Server	Server	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 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