Recorded Future®

CVE
MONTHLY

Recorded Future CVE Monthly June 2024

Executive Summary

In June 2024, Insikt Group identified fifteen high-risk vulnerabilities that defenders should prioritize for review, six of which were actively exploited in the wild to execute code remotely, elevate privileges, and reveal the source code behind scripts.

One theme worth highlighting this month was attacks exploiting vulnerabilities that have already been patched. Threat actors exploited one such vulnerability in Microsoft Windows PHP to deliver TellYouThePass ransomware to victims. In another such case, threat actors exploited an already-patched path traversal vulnerability in SolarWinds Serv-U file transfer server. Additionally this month, threat actors exploited a new zero-day flaw in the MOVEit Transfer SFTP.

Another trend this month was vulnerabilities exploited in the wild after security researchers publicly released proof-of-concept (PoC) exploit scripts. This is indicative of the ongoing debate in the security community about the most effective way to disclose and patch vulnerabilities. While enterprises struggle to patch vulnerabilities in real-time, releasing proof-of-concept (PoC) exploit code within days of vulnerability disclosure likely proves more advantageous to threat actors than to defenders.

Key Findings

- Insikt Group identified six high-risk vulnerabilities that were exploited in the wild this month; they were found in software from Google, Linux, Microsoft, Check Point, SolarWinds, and MOVEit.
- Since June 6, 2024, threat actors have been actively exploiting CVE-2024-4577, a previously patched remote code execution (RCE) vulnerability affecting all PHP versions for Microsoft Windows.
- GreyNoise reported on June 18, 2024, that threat actors were actively exploiting a path traversal vulnerability in SolarWinds' Serv-U file transfer server: CVE-2024-28995. (Previously disclosed and patched on June 5, 2024.) Older versions of Serv-U are also reportedly affected, but these versions are unsupported by SolarWinds. Rapid7 published a single-line PoC exploit script just six days after CVE-2024-28995 was disclosed. Rapid7 noted publicly that the flaw was "trivially" easy to exploit, which likely contributed to the exploitation of the flaw in the wild.
- Progress Software patched two critical vulnerabilities, CVE-2024-5805 and CVE-2024-5806, affecting its MOVEit File Transfer software. Both vulnerabilities involve authentication bypass issues, allowing threat actors to gain unauthorized access to internal systems if exploited.
- The Cybersecurity and Infrastructure Security Agency (CISA) added CVE-2024-1086, a use-after-free vulnerability in the Linux Kernel, to its Known Exploited Vulnerabilities (KEV) catalog on May 30, 2024. CVE-2024-1086 was initially disclosed in April 2024 when a PoC script was published for it, but exploits were not observed until more recently. Threat actors can abuse the flaw to elevate local privileges.
- Check Point discovered and patched a high-severity Security Gateway information disclosure vulnerability on May 28, 2024, tracked as CVE-2024-24919, after detecting an increase in attacks on virtual private network (VPN) devices. The vulnerability enables threat actors to access internet-connected gateways that have remote access VPN or mobile access enabled.
- CISA added CVE-2024-32896, a vulnerability affecting Google Pixel, to its Known Exploited Vulnerabilities (KEV) catalog. There are limited public details about exploitation of the vulnerability at this time.

Detailed Analysis

Update: Threat Actors Actively Exploit Critical Remote Code Execution Vulnerability in all PHP Versions For Windows

Since June 6, 2024, threat actors have been actively exploiting CVE-2024-4577, a previously patched remote code execution (RCE) vulnerability affecting all PHP versions for Microsoft Windows. According to telemetry data shared by Palo Alto's Unit 42 on June 12, 2024, threat actors executed malicious code using the `auto_prepend_file` function, enabling RCE on targeted machines and revealing sensitive source code. CVE-2024-4577 stems from an oversight in handling character encoding conversions, specifically the "Best-Fit" feature on Windows when PHP operates in Common Gateway Interface (CGI) mode.

Researchers published PoC scripts to exploit CVE-2024-4577 between June 7 and 9. Shadowserver also observed multiple exploit attempts targeting CVE-2024-4577 via its honeypot servers during this time period. Imperva revealed that a threat actor exploited the vulnerability to deliver the TellYouThePass ransomware, using "a known exploit for CVE-2024-4577 to execute malicious PHP code on a target system", which included a VBScript to execute the ransomware in memory. Subsequently, the ransomware established a connection with a command-and-control (C2) server and encrypted and exfiltrated sensitive files.

A researcher at Devcore initially discovered the vulnerability on May 6, 2024, noting that the PHP development team released the first version of the patch on May 16. Devcore said on June 6 that "the vulnerability affects XAMPP for Windows by default". PHP released the latest PHP version (8.2.20) on June 6, 2024.

Patched SolarWinds Serv-U Vulnerability Exploited in the Wild

GreyNoise reported on June 18 that threat actors were actively exploiting a path traversal vulnerability in SolarWinds' Serv-U file transfer server, tracked as CVE-2024-28995. GreyNoise used a honeypot to identify both manual and automated attempts to exploit the vulnerability. CVE-2024-28995 can be exploited via a GET request that references InternalDir and InternalFile, intended to fetch files without path-traversal segments (`../`). An example of this is `GET /?InternalDir=/../../../../windows&InternalFile=win.ini HTTP/1.1`. The path-traversal filter only checks for slashes "`/`" on Linux and "`\`" on Windows, then later fixes the slashes. This allows for incorrect slashes to pass inspection.

The vulnerability was initially disclosed by SolarWinds (along with a patch) on June 5, 2024. The following Serv-U versions are vulnerable:

- Serv-U FTP Server 15.4
- Serv-U Gateway 15.4
- Serv-U MFT Server 15.4
- Serv-U File Server 15.4.2.126 and earlier

Older versions of Serv-U are also reportedly affected, but these versions are unsupported by SolarWinds. Rapid7 published a PoC exploit code on June 11, 2024, and referred to the vulnerability as "trivially" easy to exploit.

Threat Actors Actively Exploit New MOVEit Transfer Vulnerability
On June 25, 2024, Progress Software patched two critical vulnerabilities, CVE-2024-5805 and CVE-2024-5806, affecting its MOVEit File Transfer software. Both vulnerabilities involve authentication bypass issues, potentially allowing threat actors to gain unauthorized access to these systems. The UK government-funded Shadowserver Foundation recorded instances of exploitation attempts of CVE-2024-5806 on June 25, 2024, shortly after a proof-of-concept (PoC) exploit was disclosed by security researchers at the cybersecurity firm watchTowr. On June 26, 2024, the German government also warned that it was seeing the exploitation of CVE-2024-5806 and urged affected organizations to patch their systems.

CVE-2024-5806 is a critical authentication bypass vulnerability in the MOVEit Transfer SFTP service. Threat actors can exploit this vulnerability if "they possess knowledge of an existing username, the account can authenticate remotely, and the SFTP service is exposed". Progress Software has issued patches for affected versions: MOVEit Transfer (SFTP Module) 2023.0.x (fixed in version 2023.0.11), 2023.1.x (fixed in version 2023.1.6), and 2024.0.x (fixed in version 2024.0.2). For additional information about this vulnerability and watchTowr's PoC exploit and description, please refer to this TTP Instance in the Recorded Future Intelligence Cloud.

CVE-2024-5805 is a critical authentication bypass vulnerability in MOVEit Gateway software version 2024.0.0. Per Rapid7, earlier versions of MOVEit Gateway software are unlikely to be susceptible to attack, which likely reduces the potential attack surface. Progress Software has released a patch in version 2024.0.1, and organizations running MOVEit Gateway should apply this update urgently. MOVEit Gateway, an optional component, is intended to proxy traffic to and from MOVEit Transfer instances. This vulnerability does not affect MOVEit Cloud customers since MOVEit Gateway is not used in that environment.

CISA Adds Linux Kernel Use-After-Free Vulnerability To Known Exploited Vulnerability Catalog
The US Cybersecurity and Infrastructure Security Agency (CISA) added CVE-2024-1086 to its Known Exploited Vulnerabilities (KEV) catalog on May 30, 2024. CVE-2024-1086 is a use-after-free (UAF) flaw in the "`nft_verdict_init()`" function of the Linux kernel's Netfilter subsystem, affecting CloudLinux operating system (OS) versions 6h and 7. This vulnerability arises from mishandling positive values as drop errors within the hook verdict during network packet evaluation. If the system confuses an "`NF_DROP`" action for "`NF_ACCEPT`", it could mistakenly trigger the "`nf_hook_slow()`" function, responsible for processing network packets, to attempt to free a memory address that has already been freed. Successful abuse enables threat actors to gain local privilege escalation on the affected system.

TuxCare released patched CVE-2024-1086 on April 10, 2024, and urged users to promptly update affected CloudLinux 6h and CloudLinux 7 to the latest versions.

Update: Check Point Patches Zero-Day Information Disclosure Flaw CVE-2024-24919; Exploit Attempts Detected Since Early April 2024
Check Point discovered and patched a high-severity Security Gateway information disclosure vulnerability on May 28, 2024, tracked as CVE-2024-24919, after detecting an increase in attacks on VPN devices. The vulnerability enables threat actors to access internet-connected gateways that have remote access VPN or mobile access enabled.

According to Check Point, the vulnerability was discovered as a result of the company's investigation into unauthorized access attempts to VPN technologies. On May 24, 2024, Check Point discovered "a small number of [suspicious] login attempts" on old VPN local accounts that were using outdated

password-only authentication measures. Then, on May 27, 2024, Check Point observed an "increased interest of malicious groups in leveraging remote-access VPN environments". By May 28, 2024, Check Point stated that they "found the root cause for these [attacks]" (likely referring to CVE-2024-24919) and subsequently released a patch for the vulnerability.

In Check Point's Frequently Asked Questions (FAQ) page, its initial telemetry data showed that exploitation attempts occurred on April 30, 2024. However, further investigation found that exploitation attempts actually date back to April 7, 2024. Moreover, the company has so far identified 51 unique IP addresses that attempted to exploit CVE-2024-24919. CheckPoint shared in its advisory a script that allows users to check for vulnerable instances of CVE-2024-24919.

Products affected by CVE-2024-24919 are as follows: CloudGuard Network, Quantum Maestro, Quantum Scalable Chassis, Quantum Security Gateways, and Quantum Spark Appliances. The affected versions include R80.20.x, R80.20SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x, and R81.20. Check Point warned that successful exploitation of the vulnerability can allow threat actors to access sensitive data from vulnerable devices. Additionally, after exploiting the vulnerability, threat actors can potentially move laterally across the network and subsequently gain administrative privileges.

Security firm Censys revealed that as of May 31, 2024, more than 13,800 aforementioned products are publicly exposed to the internet, but not all have vulnerable instances of CVE-2024-24919. Of the 13,800, Quantum Spark Gateways have the highest number (12,598) of publicly exposed instances, followed by Quantum Security Gateways (1,063) and CloudGuard Network Security instances (141). According to Censys, a majority of the affected hosts are geographically located in Japan, followed by Italy. Cybersecurity company Mnemonic observed that on April 31, 2024, threat actors exploited the vulnerability to harvest Active Directory credentials from customer environments. Threat actors subsequently used those credentials to move laterally across the network.

Threat Actors Exploit Command Injection Flaw in Zyxel NAS Devices

Threat actors used a botnet that resembles Mirai to exploit CVE-2024-29973, a critical command injection vulnerability in Zyxel NAS devices, according to a report by Security Online on June 23, 2024.

On March 14, 2024, a security researcher at Outpost24 identified and reported the flaw to Zyxel, along with four other vulnerabilities of critical severity. On June 4, 2024, Zyxel disclosed the vulnerabilities, which affect Zyxel NAS326 devices with firmware versions before 5.21 and NAS542 devices with firmware versions later than 5.21. These devices are network-attached storage (NAS) solutions designed for home and small office environments that have reached the end-of-vulnerability-support stage. The other vulnerabilities are CVE-2024-29972, CVE-2024-29974, CVE-2024-29975, and CVE-2024-29976. These include backdoor account access, privilege escalation, Python code injection, and persistent remote code execution vulnerabilities.

Exploiting CVE-2024-29973 can allow threat actors to inject and execute commands remotely. This vulnerability uses a flaw in the "`setCookie`" parameter, enabling unauthorized access to the device's operating system. According to a report by Shadowserver on June 21, 2024, the exploit attempts on CVE-2024-29973 have been linked to a Mirai-like botnet, known for hijacking devices to launch distributed denial-of-service (DDoS) attacks. Zyxel has responded by releasing patches for CVE-2024-29972, CVE-2024-29973, and CVE-2024-29974 and advising users to update to the latest firmware versions, which is notable given vendors don't often patch vulnerabilities in end-of-life products. Zyxel did not release patches for CVE-2024-29975 or CVE-2024-29976, which can allow for unauthorized privilege escalation and improper information disclosure, respectively.

Outpost24's report on CVE-2024-29973 included a PoC exploit script for the flaw, but no exploits were reported until Shadowserver published its finding on June 21, 2024.

CVE Monthly Prominent Vulnerability Disclosures

Insikt Group identified 291 vulnerabilities with high to very critical risk scores for the month of June, per Recorded Future data. Insikt Group provides the associated Risk Score, which ranges from "None" (0) to "Very Critical" (90-99). These scores are "live" and are subject to change.

We highlighted fifteen of the highest-ranking vulnerabilities from our monthly dataset in the table below.

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/Component	Actively Exploited?
1	CVE-2024-32896	99	Google Pixel, Google Android	There is a way to bypass due to a logic error in the code. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is needed for abuse.	Yes
2	CVE-2024-4577	99	Microsoft Windows PHP	In PHP versions 8.1.* before 8.1.29, 8.2.* before 8.2.20, and 8.3.* before 8.3.8, when using Apache and PHP-CGI on Windows, if the system is set up to use certain code pages, Windows may use "Best-Fit" behavior to replace characters in the command line given to Win32 application programming interface (API) functions. PHP CGI module may misinterpret those characters as PHP options, which may allow a malicious user to pass options to the PHP binary being run and thus reveal the source code of scripts, run arbitrary PHP code on the server, and so on.	Yes
3	CVE-2024-1086	99	Linux Kernel	This CVE is a use-after-free vulnerability in the Linux kernel's netfilter: `nf_tables` component that can be exploited to achieve local privilege escalation.	Yes
4	CVE-2024-24919	99	CheckPoint Security Gateway	Potentially allows an attacker to read certain information on Check Point Security Gateways once connected to the internet and enabled with remote Access VPN or Mobile Access Software Blades. A Security fix that mitigates this vulnerability is available.	Yes
5	CVE-2024-21338	89	Microsoft Windows 10	Windows Kernel Elevation of Privilege Vulnerability	No

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/Component	Actively Exploited?
6	CVE-2024-29849	79	Veeam Backup Enterprise Manager	Veeam Backup Enterprise Manager allows unauthenticated users to log in as any user enterprise manager web interface.	No
7	CVE-2024-21345	79	Microsoft Windows Server	Windows Kernel Elevation of Privilege Vulnerability	No
8	CVE-2024-26229	79	Microsoft Windows CSC	Windows CSC Service Elevation of Privilege Vulnerability	No
9	CVE-2024-5806	79	Progress MOVEit	Improper Authentication vulnerability in Progress MOVEit Transfer (SFTP module) can lead to Authentication Bypass. This issue affects MOVEit Transfer versions between 2023.0.0 and 2023.0.11, between 2023.1.0 and 2023.1.6, and between 2024.0.0 and 2024.0.2.	Yes
10	CVE-2024-28995	79	SolarWinds Serv-U	SolarWinds Serv-U was susceptible to a directory transversal vulnerability that would allow access to read sensitive files on the host machine.	Yes
11	CVE-2024-30078	79	Microsoft Windows 10	Windows Wi-Fi Driver Remote Code Execution Vulnerability	No
12	CVE-2024-30080	79	Microsoft Windows Server 2019	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	No
13	CVE-2024-30103	79	Microsoft Outlook	Microsoft Outlook Remote Code Execution Vulnerability	No
14	CVE-2024-29855	79	Veeam Recovery Orchestrator	Hard-coded Jason web token (JWT) secret allows authentication bypass in Veeam Recovery Orchestrator	No

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/Component	Actively Exploited?
15	CVE-2024-29973	79	Zyxel NAS326 devices with firmware versions before 5.21 and NAS542 devices with firmware versions later than 5.21	** UNSUPPORTED WHEN ASSIGNED ** The command injection vulnerability in the "`setCookie`" parameter in Zyxel NAS326 firmware versions before V5.21(AAZF.17)C0 and NAS542 firmware versions before V5.21(ABAG.14)C0 could allow an unauthenticated attacker to execute some operating system (OS) commands by sending a crafted HTTP POST request.	No

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

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 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com