Recorded Future®

CVE
MONTHLY

Recorded Future CVE Monthly April 2024

Executive Summary

In April 2024, we identified fourteen high-risk vulnerabilities, seven of which were actively exploited in the wild to execute code remotely, achieve persistent access, move laterally, and escalate privileges. In some instances, exploitation of these vulnerabilities ultimately allowed threat actors to gain root (administrative) level access.

This month, several state-sponsored threat actors exploited vulnerabilities in enterprise perimeter devices to achieve stealthy, persistent access to enterprise networks. Threat actors were observed exploiting vulnerabilities in Palo Alto's PAN-OS (CVE-2024-3400) and Cisco's Adaptive Security Defense (ASA) software (CVE-2024-20353 and CVE-2024-20359), which provide defense for network perimeters. Additionally, this month, MITRE Corporation reported that starting in January 2024, an unspecified, sophisticated state-sponsored threat actor maintained access to MITRE's network by first exploiting two zero-day vulnerabilities in Ivanti Connect Secure virtual private network (VPN) appliances.

Once threat actors breach perimeter network devices, they can exploit their positioning between internal networks and the external internet to move laterally, intercept traffic, and exfiltrate data. Unlike client devices and software, perimeter-exposed products are less likely to have detailed logging capabilities, enabling threat actors to exploit them for access while remaining undetected. For example, MITRE stated that although it patched the two zero-day Ivanti Connect Secure vulnerabilities at the time of their disclosure, the threat actors had already achieved initial access and remained undetected for months. This event underscores that threat hunting to identify anomalous activity on perimeter devices should occur alongside patching to ensure threat actors that obtain access preceding patch implementation are sufficiently detected.

Another trend we have been tracking is the opportunistic exploitation of vulnerabilities in file transfer services, exemplified by the CrushFTP vulnerability exploited this month. Previous mass exploitation of Progress Software's MOVEit, Fortra's GoAnywhere, and Accellion FTA have demonstrated that attacks against file transfer services can have cascading downstream effects for customers. File transfer platforms are desirable targets for financially motivated threat actors since they can contain high volumes of sensitive data and offer the potential to compromise organizations at scale. For defenders, what remains is the main challenge of securing these third-party software solutions without sacrificing the integral part they play in business operations.

Key Findings

- We identified seven high-risk vulnerabilities that were exploited in the wild this month, which were found in software by vendors like Palo Alto, CrushFTP, Cisco, Microsoft, and Google.
- Although we did not see them being actively exploited, we identified four vulnerabilities associated with a public proof-of-concept (PoC) exploit code, enabling threat actors to more easily exploit the vulnerability.
- State-sponsored threat actors exploited vulnerabilities in enterprise perimeter devices — specifically, Palo Alto's PAN-OS firewall software (CVE-2024-3400) and Cisco Adaptive Security Appliances (CVE-2024-20353 and CVE-2024-20359) — to achieve stealthy, persistent access to enterprise networks.

- A vulnerability in CrushFTP's file transfer service (CVE-2024-4040) enables remote attackers to read files, gain administrative access, and perform remote code execution (RCE) on a CrushFTP server.
- Microsoft's Patch Tuesday for April 2024 patched two zero-day vulnerabilities that were actively exploited in malware attacks. One of the vulnerabilities, CVE-2024-29988, was exploited by the advanced persistent threat (APT) group Water Hydra.

Detailed Analysis

Palo Alto Networks Warns of Critical Vulnerability (CVE-2024-3400) in its PAN-OS Firewall Software, Provides Workaround Remediation Ahead of Patch Releases

On April 12, 2024, Palo Alto released a security advisory warning users of an actively exploited critical vulnerability (CVE-2024-3400, CVSS score 10.0) affecting Palo Alto Networks's PAN-OS software. PAN-OS is the operating system that powers all next-generation firewalls (NGFWs) developed by Palo Alto Networks. CVE-2024-3400 is a command injection vulnerability in the GlobalProtect feature of the PAN-OS software versions 10.2, 11.0, and 11.1. Exploitation of CVE-2024-3400 can enable a threat actor to take complete control of a vulnerable firewall device, allowing unauthenticated execution of arbitrary code with root privileges on affected firewall devices.

Security company Volexity identified exploitation of CVE-2024-3400 on April 10, 2024, when Volexity received alerts about suspicious network traffic affecting a customer's NGFW firewall via its network security monitoring (NSM) service; further investigation revealed that the device was compromised. Additional investigation by Volexity revealed that an unknown state-sponsored threat actor, tracked by Volexity as "UTA0218", began experimentally exploiting CVE-2024-3400 on March 26, 2024. Volexity identified another NGFW compromised via CVE-2024-3400 on April 11, 2024, also via alerts from its NSM service.

After remotely compromising the firewall devices, UTA0218 was able to create a reverse shell and download executables onto the device. Post-intrusion, the attacker exfiltrated configuration data from victim devices and moved laterally within the affected enterprise networks by extracting sensitive credentials.

In its disclosure on April 12, 2024, Palo Alto acknowledged that it was "aware of an increasing number of attacks" exploiting CVE-2024-3400. As of April 16, 2024, Shadowserver data found over 156,000 potentially vulnerable internet-facing Palo Alto firewall devices, representing thousands of organizations.

State-Sponsored Actors Exploiting Two Zero-Day Vulnerabilities in Cisco Adaptive Security Appliances

On April 24, 2024, Cisco Talos published findings about an espionage campaign dubbed ArcaneDoor in which an unknown threat actor, UAT4356, targeted Cisco Adaptive Security Appliances (ASA) by exploiting two zero-day vulnerabilities. While the initial access vector remains unidentified, Cisco confirmed that UAT4356 eventually chained exploitation of CVE-2024-20353 and CVE-2024-20359 to compromise the ASAs. Cisco assessed that the campaign was likely state-sponsored based on the victims affected, tradecraft employed, and use of zero-day vulnerabilities. UAT4356 targeted critical sectors such as telecommunications and energy and employed malware, including Line Dancer, a memory-resident shellcode interpreter, to execute and maintain their malicious activities. The threat actor also employed Line Runner, a persistent backdoor, to establish persistence.

After exploiting CVE-2024-20353 and CVE-2024-20359, threat actors deployed Line Dancer onto Cisco ASA devices. Line Dancer enabled extensive network surveillance, which included traffic capture, and it enabled data manipulation, which included configuration changes. Subsequently, the Line Runner backdoor was installed using the Cisco ASA device boot process and established persistence by automatically reactivating post-reboot and deleting the logs of the persistence script to minimize forensic traces, maintaining stealth through system updates. Finally, UAT4356 employed several anti-forensic measures to evade detection, including disabling syslog services, which inhibited malicious activity logging, and manipulating crash dump settings to prevent the generation of forensic evidence during system crashes.

CrushFTP Vulnerability Exploited in Attacks Targeting United States (US) Organizations
On April 15, 2024, CrushFTP privately disclosed to its customers an actively exploited zero-day vulnerability, CVE-2024-4040, affecting versions of the CrushFTP file transfer service before 10.7.1 and 11.1.0, as well as legacy 9.x versions. CrushFTP's public disclosure was released on April 22, 2024. CVE-2024-4040 is an unauthenticated server-side template injection vulnerability that enables remote attackers to read files, gain administrative access, and perform remote code execution (RCE) on a CrushFTP server. Exploit code for CVE-2024-4040 has been available since April 23, 2024, and the Cybersecurity and Infrastructure Security Agency (CISA) added CVE-2024-4040 to its Known Exploited Vulnerabilities (KEV) list on April 24, 2024. At this time, it is not publicly known which threat actors are exploiting these vulnerabilities or which organizations have been targeted.

According to Rapid7, as of April 24, 2024, approximately 5,200 instances of CrushFTP are currently exposed to the public internet and possibly vulnerable to attack. Given that this vulnerability has low barriers to exploitation and instances of CrushFTP are publicly discoverable, we recommend remediating the vulnerabilities as soon as possible. CVE-2024-4040 was patched on April 19, 2024, with the release of CrushFTP 11.0.1. For complete details, please see CrushFTP's original advisory.

Microsoft Patches Two Zero-Day Vulnerabilities That Were Actively Exploited in Patch Tuesday
Microsoft's April 2024 Patch Tuesday included security updates for 150 vulnerabilities, including fixes for two zero-day vulnerabilities that were actively exploited in malware attacks. One zero-day, CVE-2024-26234, involved a proxy driver spoofing vulnerability that used a valid Microsoft Hardware Publisher certificate. To exploit this vulnerability, an attacker needs to obtain a high level of privileges (in other words, administrative access) over the vulnerable component. The other, CVE-2024-29988, was a bypass for a previous flaw (CVE-2023-36025) and allowed attachments to bypass Microsoft Defender SmartScreen prompts. The financially motivated advanced persistent threat (APT) group Water Hydra used this vulnerability in spearphishing attacks. The update also included 67 remote code execution (RCE) bugs and addressed 26 Secure Boot bypasses.

Threat Actors Maintained Access to MITRE Networks for Three Months via Ivanti Connect Secure Vulnerabilities
MITRE reported on April 19, 2024, that starting in January 2024, an unspecified, sophisticated state-sponsored threat actor successfully breached its Networked Experimentation, Research, and Virtualization Environment (NERVE) by exploiting two zero-day vulnerabilities (CVE-2023-46805 and CVE-2024-21887) in Ivanti Connect Secure VPN appliances. NERVE is an unclassified network designed for research and development collaboration. Exploitation of CVE-2023-46805 and CVE-2024-21887 enabled the threat actors to bypass multi-factor authentication via session hijacking, compromise an administrative account, and move laterally into MITRE's VMware infrastructure. Post-intrusion, the threat actors deployed sophisticated backdoors and webshells to maintain persistence and steal credentials.

While initial reconnaissance and infection took place in January 2024, MITRE did not discover the intrusion until April 2024. MITRE followed guidances to patch CVE-2023-46805 and CVE-2024-21887 and secure their Ivanti Connect Secure VPN appliances in January 2024, but it did not detect that the threat actor had already achieved persistence on their systems.

CVE Monthly Prominent Vulnerability Disclosures

Insikt Group provides the associated Risk Score according to the Recorded Future Intelligence Cloud data, which ranges from "None" (0) to "Very Critical" (90-99). These scores continue to evolve with new analytics and sources.

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/Component	Actively Exploited?
1	CVE-2024-3400	99	PAN-OS versions 10.2, 11.0, and 11.1	This CVE is a command injection vulnerability in the GlobalProtect feature of the PAN-OS software. Exploiting CVE-2024-3400 can enable a threat actor to control a vulnerable firewall device completely, allowing the threat actor to unauthentically execute arbitrary code with root privileges on affected firewall devices.	Yes
2	CVE-2024-20359	99	Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD)	This CVE is a local code execution vulnerability in Cisco ASA and FTD software that can allow an authenticated, local attacker to execute arbitrary code with root-level privileges.	Yes
3	CVE-2024-20353	99	Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD)	This CVE is a vulnerability in the management and VPN web servers of Cisco ASA and FTD software that can allow an unauthenticated, remote attacker to force unexpected reloading on a targeted device, triggering a denial-of-service (DoS) condition.	Yes
4	CVE-2024-4040	99	CrushFTP	This CVE is an unauthenticated server-side template injection vulnerability that enables remote attackers to read files, gain administrative access, and perform remote code execution (RCE) on a CrushFTP server.	Yes
5	CVE-2024-26234	99	Various versions of Windows Server from 2008 to 2022, Windows 10 and 11 versions 1507 to 23H2	This CVE is a proxy driver spoofing vulnerability that uses a valid Microsoft Hardware Publisher certificate to execute a backdoor.	Yes
6	CVE-2024-29748	99	Google Pixel	This CVE is an elevation of privilege vulnerability that affects the Google Pixel firmware and permits threat actors to bypass factory resets. This enables persistent access to the device despite attempts to securely erase its contents.	Yes

#	Vulnerability	Risk Score	Affected Vendor/ Product	Vulnerability Type/Component	Actively Exploited?
7	CVE-2024-29745	99	Google Pixel	This CVE is an information disclosure vulnerability in the Pixel's bootloader that enables memory dumping by rebooting the device into fastboot mode, thereby allowing unauthorized access to the device's memory.	Yes
8	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.	No, but PoC exploit is available
9	CVE-2024-20295	79	Cisco Integrated Management Controller (IMC)	This CVE is a vulnerability that allows threat actors to perform command injection attacks on the underlying operating system, potentially elevating privileges to root. The vulnerability stems from insufficient validation of user-supplied input within the command-line interface (CLI) of the IMC.	No, but PoC exploit is available
10	CVE-2024-20356	79	Cisco Integrated Management Controller	This CVE is a vulnerability in the web-based management interface of Cisco IMC that could allow an authenticated, remote attacker with administrator-level privileges to perform command injection attacks and elevate their privileges to root.	No, but PoC exploit is available
11	CVE-2024-26218	78	Windows Kernel	This CVE is an Elevation of Privilege vulnerability in Windows Kernel that allows a threat actor to manipulate the content of user-mode memory between fetches. This can trigger unexpected behavior in the process creation process, which could lead to system instability.	No, but PoC exploit is available
12	CVE-2024-29204	77	Ivanti Avalanche	This CVE is a critical heap overflow vulnerability in the WLAvalancheService component of Ivanti Avalanche affects versions prior to 6.4.3. It allows unauthorized remote execution of arbitrary commands due to improper buffer management. Threat actors can exploit this flaw with minimal complexity and without requiring user interaction.	No
13	CVE-2023-6320	77	LG webOS	This CVE is a command injection vulnerability in an endpoint on webOS versions 5 and 6. Threat actors can send specially crafted requests to enable command execution as the dbus user.	No
14	CVE-2023-40000	77	LiteSpeed Technologies LiteSpeed Cache	This CVE is a cross-site scripting vulnerability in LiteSpeed Technologies LiteSpeed Cache that can allow a threat actor to inject malicious scripts into a website.	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.