

Simplify the complex

Threat Pulse

Threats • News • Phishing

*Amateurs hack systems; professionals
hack people*

– Bruce Schneier

The News

In the news week



F5 Patches Critical BIG-IP APM Zero-Day Exploited for Unauthenticated RCE on OAuth Servers

Attackers are exploiting a critical flaw in F5 BIG-IP Access Policy Manager (APM) that lets them run code on a BIG-IP system without logging in, F5 says.

The flaw, [CVE-2026-94127](#), affects only systems in which APM serves as an OAuth authorization server, issuing access tokens to applications. F5 disclosed it in [an advisory](#) on September 22 and has released engineering hotfixes.

APM is the BIG-IP module that controls how users reach an organization's applications and networks. The vulnerable setup has an APM access policy and an OAuth authorization server profile on the same virtual server, which hosts the BIG-IP address that receives the OAuth traffic. Specific malicious traffic sent to that virtual server can lead to remote code execution.

The flaw is a heap-based buffer overflow. F5 rates it 9.8 out of 10 on CVSS v3.1 and 9.3 on CVSS v4.0.

Because the malicious traffic goes to the virtual server itself, limiting access to the BIG-IP management interface does not protect against this flaw. BIG-IP systems in Appliance mode are also vulnerable.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added the flaw to its Known Exploited Vulnerabilities (KEV) catalog on September 22. It gave federal civilian agencies until September 25 to apply F5's mitigations, under [a directive CISA issued in June](#).

[Read more >](#)

Other news highlights

[A Leaked GitLab Issue Email Address Lets Anyone Push Code and Run CI Jobs as You](#)

—

[Attackers Exploit WordPress CVE-2026-87902 Within Hours of Disclosure](#)

—

[Attackers Use Malicious Terraform Providers to Deliver Go Malware via HashiCorp Registry](#)

—

[MikroTrick Chain Let Attackers Take Over MikroTik Routers Without a Password or SSH Key](#)

The News

Top of the news



Check Point Warns of Management Server Zero-Day Exploited in Targeted Attacks

Attackers exploited a previously unknown flaw in Check Point's Security Management Server in a handful of targeted attacks on July 23, the company said.

The flaw, CVE-2026-93616, allows an attacker who can access the server's web service to run scripts on it without logging in. Check Point released a fix on September 22 for the server that controls firewall policies for the Check Point gateways it manages.

Separately, Check Point said attackers have been trying since September 12 to exploit a VPN flaw it fixed on September 9. The attempts, against a flaw tracked as CVE-2026-85102, have targeted customers of Spark, Check Point's firewall line for small businesses. When the fix came out, Check Point had no evidence the flaw was being exploited.

CVE-2026-93616 is a path traversal bug in the management server's web service. The service does not properly limit which files and folders a request can reach.

An attacker can use it to upload scripts to the server and then run them. Check Point rated it 9.8 out of 10 on the CVSS scale in the CVE record for the flaw.

[Read more >](#)

Other news highlights

[WordPress Issues Patch for Critical Flaw That Can Enable Code Execution on Some Servers](#)

[Researcher Drops BigDiskBuster Zero-Day PoC That Blocks Microsoft Defender Updates](#)

[New Linux Kernel Flaw Gives ARM64 KVM Guests Read-Write Access to Host Memory](#)

[SharePoint Flaw Initially Listed as Spoofing by Microsoft Enables Authenticated RCE](#)

Geo-Politics

News from around the world



Other news highlights

[Poland says fire at Starlink station is sabotage as Denmark warns of rising Russian threat](#)

—

[North Korea uses remote IT worker to clandestinely earn NZ currency](#)

—

[Russia reports thousands of cyberattacks on election infrastructure during vote](#)

—

[OpenAI gives cyber defence tools to Ukraine](#)

Jade Sleet Linked to Indian IT Provider Breach With FLATROOF and ROOFDECK Backdoors

The North Korean threat actor known as Jade Sleet has been attributed to the compromise of an India-based "much smaller organization" in the information technology (IT) services industry, once again highlighting how the adversary continues to target developers to breach target networks.

Cybersecurity company SentinelOne, which [disclosed](#) details of the activity, said it involved the use of Apple macOS backdoors tracked as FLATROOF (aka [Gaslight](#)) and ROOFDECK, both of which were previously observed in the [March–April 2026 attack](#) on [KelpDAO's LayerZero bridge](#).

Jade Sleet, also tracked under the monikers PUKCHONG, Slow Pisces, TraderTraitor, and UNC4899, has a [history of targeting](#) the Web3 sector for cryptocurrency heists. In early 2025, the hacking group was [tied](#) to the [theft of about \\$1.5 billion](#) from Bybit's cold wallet infrastructure following a supply chain compromise of Safe{Wallet}'s developer environment.

"Jade Sleet mostly targets users associated with cryptocurrency and other blockchain-related organizations, but also targets vendors used by those firms," Microsoft-owned GitHub [noted](#) in July 2023.

[Read more >](#)

Breaches

Security Breaches this week



Other news highlights

[BigCommerce Data Stolen via Ribon Apps Hack](#)

—

[CrowdSec Confirms Source Code Stolen in Supply Chain Attack](#)

—

[ShinyHunters Claims FBI Hack, Demands Retraction of Threat Report](#)

—

[23 Million User Records Compromised in Gyazo Data Breach](#)

Astrana Health Data Breach Impacts Private, Confidential Information

Astrana Health says private and confidential information was stolen from its servers after employees were targeted in a social engineering attack.

Astrana Health is a California-based physician-centric healthcare management company that provides back-office services, including claims and billing.

The incident involved the company's subsidiary Astrana Health Management, according to a [filing](#) with the US Securities and Exchange Commission (SEC).

Hackers used social engineering to access the company's servers, impersonating Astrana Health personnel and spoofing its main phone number to contact employees.

After detecting the attack, the company engaged a third-party cybersecurity firm, notified the relevant authorities and its partners, and launched an investigation.

In response to the intrusion, Astrana Health rotated credentials, restricted remote access tools, rebuilt certain systems from clean backups, and improved its monitoring, logging, and detection.

[Read more >](#)

Vulnerabilities

Vulnerabilities & Exploits



CVE-2026-87902 – An unauthenticated attacker can make ``get_page_template()`` page-template resolution include a chosen readable local `.php`` file outside the active theme directories. If relevant pre-conditions for both the server and the active theme are met, this can lead to RCE.

CVSS score: 8.1

CVE-2026-94127 – When a BIG-IP APM access policy and an OAuth profile are configured on a virtual server, specific malicious traffic can lead to remote code execution (RCE). This vulnerability is only present when BIG-IP APM is configured as an OAuth Authorization Server. Deployments using APM strictly as an OAuth Client / Resource Server (without OAuth authorization server profiles configured) are not affected by this vulnerability.

CVSS score: 9.3

Last weeks recaps

CVE-2026-76460 –

A vulnerability in an API of Cisco Identity Services Engine (ISE) could allow an unauthenticated, remote attacker to bypass authentication. This vulnerability is due to insufficient authentication control on an API endpoint. An attacker could exploit this vulnerability by sending a crafted request to an affected API endpoint. A successful exploit could allow the attacker to gain unauthorized access to the affected device by bypassing the web-based management interface.

CVSS 10.0

–

CVE-2026-58704 – In Cellular Modem, there is a possible permission bypass due to a logic error in the code. This could lead to remote (proximal/adjacent) escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.

CVSS 10.0

Ransomware

Weekly Ransomware Roundups



Overview

In August 2026, ransomware activity recorded a total of 1165 victims globally, marking a 22.1% increase from the 954 victims reported in July 2026

Target industries

In August 2026, ransomware attacks intensified across nearly every major confirmed sector, with Manufacturing overtaking Professional Services to claim the top position for the first time in the current reporting cycle. Manufacturing recorded the highest confirmed victim count at 185, up 21.7% from July's 152

Target country

The United States accounted for 414 victims, representing approximately 35.5% of globally attributed incidents and remaining the dominant target geography.

Top Group

Qilin recorded 164 victims, retaking the top position after trailing TheGentlemen for two consecutive months. The group's claimed victims remain concentrated in Manufacturing, Professional Services, and Technology, spanning more than 100 countries, and its resurgence has been linked by researchers to continued exploitation of a VPN authentication-bypass flaw first observed in May 2026.

Top Threat Actors

Qilin

Qilin is a ransomware-as-a-service operation linked to Russia, encrypting and stealing data for ransom. Active since October 2022, it has targeted organizations like The Big Issue and Yanfeng.

-

The Gentlemen

The Gentlemen (also tracked as Storm-2697) is a fast-growing, financially motivated Ransomware-as-a-Service (RaaS) and double-extortion threat group active since mid-2025.

-

Clop

is a prominent cybercriminal organization and ransomware variant active since 2019. It is linked to the Russian-speaking threat collective known as TA505

Phishing

Phishing news this week



Corp MDM Spyware Targets Logistics Firms, Steals New SMS and Redirects Calls

The logistics sector has become the target of a new malicious cyber campaign that distributes an Android spyware codenamed Corp MDM.

According to Have I Been Squatted, the campaign uses fake Google Play pages branded as CEVA and TKW Logistics to distribute an Android Package Kit (APK) file that's dressed up as a system service. The delivered app has the package name "com.corp.mdm" Corp MDM is a "compact surveillance implant designed to exfiltrate newly received SMS content, divert calls, and maintain a hidden foreground service," security researcher Ben Folland [said](#).

The malware has been described as narrow by design, lacking in spyware functions typically observed in commercial Android spyware. It's suspected that the threat actor behind the campaign used artificial intelligence (AI) during the development phase, given the presence of bugs that interfere with its capabilities.

In addition, the activity is said to be part of a broader campaign targeting the logistics sector using credential phishing and Windows-based malware.

[Read more >](#)

Other news highlights

[Microsoft Takes Down EvilTokens Device-Code Phishing Service Tied to 12,000 Inbox Compromises](#)

[SideCopy Broadens India Targeting to Academia With ReverseRAT Spear-Phishing](#)

[RatHat Android Malware Abuses ADB to Retain Shell Access After Uninstall](#)

[Chinese Hackers Exploit Chrome-Windows Zero-Day Chain to Deploy CLEANPULP Malware](#)