Simplify the complex

Threat Pulse

Threats • News • Phishing

Amateurs hack systems; professionals hack people

– Bruce Schneier

SCC Threat Pulse | AUG | Vol.2

The News

In the news week

Attackers Exploit SharePoint Authentication Bypass After Public PoC Release

Threat actors have begun to exploit a newly disclosed Microsoft SharePoint vulnerability following the release of a proof-of-concept (PoC) code.

The vulnerability in question is CVE-2026-55040 (CVSS score: 9.1), which refers to a critical security feature bypass that stems from weak authentication. It was patched by Microsoft as part of its July 2026 Patch Tuesday updates.

"The authentication feature could be bypassed as this vulnerability allows impersonation," Microsoft said in an advisory for the flaw last month. "Exploiting this vulnerability could allow an attacker to disclose files and modify data, but the attacker cannot impact the availability of the system."

According to Defused Cyber, threat actors are leveraging a PoC exploit released by Rapid7 earlier this week, once again indicating fresh flaws are being rapidly abused in real-world attacks.

Read more ›

Other news highlights

AmnesiaStealer Hijacks Chromium Sessions to Give Attackers Live Browser Control on macOS

_

737 Chrome VPN Extensions Caught Routing Traffic Through Proxies. Check If You Have One

_

Adobe Patches Three CVSS 10.0 ColdFusion and Campaign Classic Flaws

_

Attackers Exploit VMware vCenter Vulnerability to Gain Persistent Remote Access

The News

Top of the news

Microsoft Patches 398 Flaws Including a Windows Driver Zero-Day Under Active Attack

Microsoft released its monthly security updates on Tuesday, and one of the flaws it closed is already being used in attacks.
The bug sits in a core Windows kernel driver that handles network socket operations. An attacker with code already running on a machine can use it to escalate to SYSTEM. That patch goes out first.
The flaw is tracked as CVE-2026-68820 (CVSS score: 7.0) and is the only one in this month's release Microsoft flags as under active exploitation. Exploitation depends on triggering a race condition in the driver. Microsoft has not publicly attributed the exploitation. Check Point Research says Lazarus used the zero-day in its Operation Dream Job campaign.
Four other flaws in the release need nothing at all from the victim: no account, no password, no click. They affect Windows DNS Server, Windows Deployment Services, Microsoft's implementation of the QUIC transport protocol, and High Performance Computing (HPC) Pack, and each carries a CVSS score of 9.8. None was flagged as exploited when the updates shipped.

Read more ›

Other news highlights

Cisco ASA and FTD Flaw Exploited in the Wild Can Trigger Remote DoS

–

ShieldBreak Zero-Day PoC Claims Microsoft Defender Patch Bypass With SYSTEM Access

–

SAP Commerce Cloud Flaw Could Let Unauthenticated Attackers Execute Arbitrary Code

–

Malicious LiteLLM Releases Tied to Trivy Hack May Have Exposed 2,100+ Organizations

Geo-Politics

News from around the world

North Korean Remote Workers Are Infiltrating Government and Businesses: How to Expose Them Before Hiring

Companies are used to thinking about attackers as outsiders trying to break in.
North Korean IT workers flip that model. They apply for jobs, pass interviews, receive legitimate credentials, and can end up inside the same systems companies spend millions trying to protect.
That risk is no longer theoretical. The FBI is now investigating a North Korean remote IT worker who reportedly worked for a U.S. federal agency.
For CISOs, the priority is clear: spot the warning signs before a fraudulent hire becomes trusted access. A recent joint investigation by Mauro Eldritch (BCA LTD), Heiner García (NorthScan), and ANY.RUN showed what this looks like from inside the operation.Researchers deliberately hired suspected DPRK developers linked to Lazarus Group and gave them what looked like ordinary virtual desktops. In reality, they were controlled ANY.RUN Sandboxes, capturing their activity in real time.

Read more ›

Other news highlights

Researchers Built a Fake Crypto Startup and Hired Three Suspected North Korean IT Workers

—

China-Linked Hackers Deploy New StormEncryptor Ransomware, Likely via N-central Flaw

—

German secret service upgrade gives ‘fighting chance’ against Iranian and Russian cyber attacks

—

Taiwan says it was hit by ‘abnormal’ AI-assisted cyber-attack

Breaches

Security Breaches this week

Hackers Breach Polish Power Plant Controls via Private Cellular Network and Shut Turbine

Attackers shut down a steam turbine and the process-water treatment system at a Polish combined heat and power plant by coming in over the private cellular network the local grid operator uses to reach remote equipment.

The plant supplies heat to roughly 50,000 residents. Recovery began at about 7:30 a.m. while the intruders were still active inside the network, and customers lost neither heat nor electricity.

CERT Polska disclosed the December 2025 incident on August 8 after an investigation lasting more than three months. Poland's prime minister had said in January that two CHP plants were hit. This is the second.

The route ran through a private APN, or access point name: a dedicated cellular data network managed by the distribution system operator. A configuration that allowed arbitrary devices on that APN to communicate with one another let the attacker pivot from a compromised wind-farm network to a controller at the CHP plant.

Read more ›

Other news highlights

Ceva Logistics Operations Disrupted by Cyberattack

–

Interpol Leverages Global System to Curtail Fraud Payments

–

'Jewelbug' APT Balances State Espionage & Cryptocurrency Theft

–

Ransomware Hits Colombian Justice Ministry Days Before Presidential Transition

Vulnerabilities

Vulnerabilities & Exploits

CVE-2026-48362 – ColdFusion is affected by an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability that could result in arbitrary code execution in the context of the current user. An attacker could exploit this vulnerability to execute arbitrary code. Exploitation of this issue does not require user interaction. Scope is changed.

CVSS score: 10.0

CVE-2026-59310 – VMware vCenter contains a directory traversal vulnerability in the Syslog server. A malicious actor with network access to vCenter may exploit this issue to execute arbitrary code.

8

CVSS score: 9.4

Last weeks recaps

CVE-2026-58073 – A vulnerability in Veeam Service Provider Console allowing an unauthenticated attacker to impersonate a managed agent and obtain that agent's credentials.

CVSS 9.5

–

CVE-2026-58048 – Improper preservation of SQL mode when renaming databases in cPanel allows execution of SQL in root context.

CVSS 9.5

Ransomware

Weekly Ransomware Roundups

Overview
In July 2026, ransomware activity recorded a total of 954 victims globally, marking a 34.9% increase from the 707 victims reported in June 2026

Target industries
In July 2026, ransomware activity recorded a total of 954 victims globally, marking a 34.9% increase from the 707 victims reported in June 2026

Target country
The United States remained the most targeted country in July 2026, accounting for 318 victims and approximately 33% of globally attributed incidents

Top Group
TheGentlemen recorded 177 victims, taking the top position after trailing Qilin last month. The group operates a fully featured RaaS platform offering affiliates a 90% revenue share — among the highest in the underground market — a structure designed specifically to draw experienced operators away from competing program

Top Threat Actors

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.

–

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.

–

DeadLock

DeadLock is a financially motivated ransomware group active since mid-2025. The group is known for utilizing decentralized infrastructure—such as Polygon blockchain smart contracts—to dynamically manage command-and-control proxy URLs and evade traditional network blocking.

Phishing

Phishing news this week

WindRelay Android Malware Turns Victims' Phones Into NFC Relays for Payment Fraud

A previously unseen Android near field communication (NFC) relay malware family dubbed WindRelay is being deployed in conjunction with a known remote access trojan (RAT) called SpyNote as part of a contactless payment fraud scheme.

The purpose-built malware, according to Group-IB, is designed to capture live card data via NFC and transmit it to fraudsters in real time. It was first detected in the wild in late August 2025.

"SpyNote's Accessibility Service access lets the fraudster sideload and activate the NFC app silently, with no screen sharing ever triggered," researchers Alexander Grabko, Konstantinos Angelopoulos, Pavlos Gaitanis, and Bruno Bijelić said.

These attacks typically work by luring prospective targets via phishing, smishing, or vishing scams into sideloading a malicious app. Once installed, the threat actor abuses SpyNote's remote access to install the NFC relay malware without any further user interaction.

Read more ›

Other news highlights

Kimsuky Builds Offline AI Stack to Boost Phishing and Automate Malware Development

–

Lazarus Exploits Windows Zero-Day to Gain SYSTEM Access and Deploy Backdoor

–

Delta probes Wi-Fi deauth attack on flight carrying DEF CON attendees

–

Nearly 14,000 crypto holders face security risk after data breach