Simplify the complex

Threat Pulse

Threats • News • Phishing

Amateurs hack systems; professionals hack people

– Bruce Schneier

SCC Threat Pulse | SEP | Vol.2

The News

In the news week

Microsoft Patches Record 974 Flaws, Including Two Exploited Windows Zero-Days

Microsoft on Tuesday broke Patch Tuesday records by addressing an earth-shattering 974 vulnerabilities spanning its software portfolio, including two flaws that it said have been actively exploited in the wild.
These include 723 flaws in Windows, 111 in Office and Office 2016, 62 in SQL, and 22 in Developer Tools. Of these, over 110 shortcomings have been assigned a critical severity rating. Three prominent vulnerability types, namely privilege escalation, remote code execution, and information disclosure, account for nearly 90% of the flaws patched this month. Along with Microsoft's fixes for 25 non-Microsoft CVEs, the update brings the total number of vulnerabilities resolved to 999.

September's record-setting security updates come after Microsoft patched 457 vulnerabilities in August, 663 in July, 220 in June, and 161 in May.

The two vulnerabilities that have come under active exploitation are listed below:

- CVE-2026-85880 (an ALPC heap-based buffer overflow)
- CVE-2026-81963 (a Windows Update Stack improper link resolution flaw)

Both carrying a CVSS score of 7.8 and allowing local attackers with low-level access to gain full SYSTEM privileges.

Read more ›

Other news highlights

SAP Patches CVSS 10.0 Kernel Flaw Enabling Unauthenticated Remote Code Execution

–

Researcher Drops New Microsoft Defender PoC Showing ShieldBreak Patch Can Be Bypassed

–

New cPanel Flaw Lets a Hosting Account With Mail Privileges Run Code as Root

–

F5 BIG-IP APM Malware Injects a PHP Web Shell Into Memory, Evading Disk Scans

The News

Top of the news

Chrome V8 Zero-Day Exploited in the Wild Enables Code Execution Inside Sandbox

Google on Thursday released updates to patch 230 security vulnerabilities, including one that has come under active exploitation in the wild.

The medium-severity vulnerability, assigned the CVE identifier CVE-2026-87491 (CVSS score: N/A), has been described as an out-of-bounds bug in V8, Chrome's JavaScript and WebAssembly engine.

"Out-of-bounds write in V8 in Google Chrome prior to 153.0.8010.36 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page," reads a description of the flaw on the NIST National Vulnerability Database (NVD). Google acknowledged it is "aware that an exploit for CVE-2026-87491 exists in the wild," but has not disclosed any additional specific information related to how it's being weaponized in real-world attacks and who is behind them.

With the latest development, Google has addressed a total of seven actively exploited Chrome zero-days since the start of the year. This includes CVE-2026-2441, CVE-2026-3909, CVE-2026-3910, CVE-2026-5281, CVE-2026-11645, and CVE-2026-85046.

Read more ›

Other news highlights

N-able N-central Pre-Auth RCE Flaw Exploited in the Wild

–

Adobe Patches Magento Zero-Day Exploited to Deploy Rust Backdoor and PHP Web Shell

–

WeChat Zero-Click Worm Took Over Accounts on iPhone and Android via Incoming Calls

–

Autonomous AI Agents Compromise Thousands of Credentials in Under Six Hours

Geo-Politics

News from around the world

Slim Spider Steals Crypto Custody Secrets From Brazilian Financial Institution

A previously undocumented financially motivated threat actor has been linked to attacks targeting Brazilian financial institutions since at least March 2026.
Cybersecurity company CrowdStrike is tracking the Brazil-based activity cluster under the name Slim Spider.

Slim Spider has been observed orchestrating a multi-stage intrusion at a Brazil-based financial institution in late March 2026, setting its sights on the entity's cryptocurrency assets and instant payment accounts.

As part of the attack, the e-crime group is said to have developed custom Bash scripts that query the cloud instance metadata to steal temporary cloud credentials over socket connections.
Upon establishing access to the organization's cloud environment, the threat actor enumerated all available secrets stored in the cloud credential manager and used the "sed" command to clone and modify secret-extracting scripts. The approach specifically focuses on credentials tied to digital financial assets.

Read more ›

Other news highlights

Russian hackers may have used fake CAPTCHA to hack Ukrainian government computers

—

Chinese hackers are running AI on stolen networks to avoid detection

—

North Korea-linked Hackers Hide a Backdoor Inside HAProxy

—

‘Disposable’ IP Firms in Serbia, Montenegro Obscure Origins of Russian Cyber Meddling

Breaches

Security Breaches this week

Mathspace Data Breach Exposes Over 1 Million People

The incident, it says, was discovered last week, roughly three weeks after hackers compromised its self-hosted Metabase instance using a known vulnerability.

The security defect, tracked as CVE-2026-72898 (CVSS score of 10/10) and described as an SQL injection issue, was patched on August 6, after it had been exploited in the wild as a zero-day.

Shortly after the patches were released, the notorious extortion group ShinyHunters claimed responsibility for hacking Metabase.

Mathspace failed to escalate Metabase's critical advisory to prioritize patching and upgraded its instance on August 29, more than two weeks after hackers hit it.

Furthermore, Mathspace did not complete the compromise checks Metabase had recommended, and did not identify the intrusion upon applying the update.Mathspace has taken its Metabase instance offline, revoked API keys, disabled the database access accounts, changed passwords, and exported the logs for investigation.

The data breach impacts 1,079,819 students, teachers, staff, and parents/guardians from Australia and New Zealand.

Hackers downloaded names, user IDs, usernames, email addresses, email verification status, time zone, country, date joined, and last login and active dates.

The platform warns that the threat actors may use the stolen information to mount phishing attacks, urging the potentially affected individuals to treat with extreme caution any unsolicited communication containing accurate references to the incident.

Read more ›

Other news highlights

OpenAI Agents Took Over Wiki Site Before Hugging Face Attack

–

ClickFix Campaigns Abuse Legitimate Services for Persistent Access

–

Berlin Responds After Data Leaked by Cyber Extortion Group

–

Suspected Russian Account Takeover Hacker Held in Atlanta

Vulnerabilities

Vulnerabilities & Exploits

CVE-2026-85046 - Type confusion in V8 in Google Chrome prior to 152.0.7977.82 allowed a remote attacker to execute arbitrary code inside the sandbox via a crafted HTML page

CVSS score: 8.8

CVE-2026-75650 - Adobe Commerce is affected by an Improper Neutralization of Special Elements Used in a Template Engine 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-2026-69730 - is a remote code execution flaw in Windows DNS Server, affecting systems where the DNS role is installed (typically domain controllers, but also standalone DNS servers). An attacker can send a malicious DNS query or crafted packet that triggers memory corruption inside the DNS service, allowing them to execute arbitrary code with SYSTEM privileges.

CVSS score: 9.8

Last weeks recaps

CVE-2026-6875 - ServiceNow has addressed a remote code execution vulnerability that was identified in the ServiceNow AI platform. This vulnerability could enable an unauthenticated user, in certain circumstances, to execute code within the ServiceNow platform. ServiceNow addressed this vulnerability by deploying a security update to hosted instances.

CVSS 9.5

_

CVE-2026-82222 - Deserialization of Untrusted Data vulnerability in Liquid Web / StellarWP GiveWP allows Object Injection. This issue affects GiveWP: from n/a through 4.16.7.1.

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

Fake IT Calls Target Executives in Microsoft 365 Data Theft and Extortion Attacks

Threat hunters have disclosed details of a widespread data theft and extortion threat cluster that's targeting Microsoft 365 and other software-as-a-service (SaaS) offerings through information technology (IT) help desk vishing, adversary-in-the-middle (AitM) token theft, and residential-proxy sign-ins.

The activity, which mainly singles out directors, vice presidents, and other executive staff, is being tracked by Arctic Wolf under the moniker PREY-0058. The operation shares significant tradecraft similarities with a data extortion group that Google-owned Mandiant calls UNC6671.

It also said that the data extortion threat actor known as Cinder likely represents yet another rebrand or a possible continuation of Pink operations, citing overlaps between organizations listed on the Cinder leak site and those connected to Pink.

It's worth noting that the ever-evolving labels do not correspond to a single proven actor identity, but rather an amorphous set of affiliates, splinter crews, or groups using the same underlying phishing infrastructure, as indicated by Google early last month.

Read more ›

Other news highlights

Rogue ScreenConnect Clients Spread Four-Stage VBScript Chain to Newly Connected Hosts

–

Phishing Campaign Sends Millions of Emails Using Invisible Unicode to Evade Filters

–

New Phishing Attack Creates Malicious Pages Inside the Victim's Browser

–

BigBear Microsoft 365 phishing service bypassed MFA at 258 organizations