

Simplify the complex

Threat Pulse

Threats • News • Phishing

*Amateurs hack systems; professionals
hack people*

– Bruce Schneier

The News

In the news week



Cisco Warns of New Zero-Day ISE Auth Bypass (CVSS 10.0) Exploited in Active Attacks

Cisco has warned of a fresh maximum-severity security flaw impacting Identity Services Engine (ISE) that has come under active exploitation.

The vulnerability, tracked as [CVE-2026-76460](#) (CVSS score: 10.0), could allow an unauthenticated, remote attacker to bypass authentication.

"This vulnerability is due to insufficient authentication control on an API endpoint," Cisco said. "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." The issue affects Cisco ISE and Cisco ISE Passive Identity Connector (ISE-PIC), regardless of device configuration. It has been addressed in the following versions –

- 3.1 – Fixed in 3.1 Patch 12
- 3.2 – Fixed in 3.2 Patch 11
- 3.3 – Fixed in 3.3 Patch 12
- 3.4 – Fixed in 3.4 Patch 7
- 3.51 – Fixed in 3.5 Patch 4

Cisco said it's "aware of active exploitation of this vulnerability," urging customers to upgrade to a fixed software release to counter the threat

Other news highlights

[Attackers Exploit Issabel Framework Flaw Enabling Unauthenticated OS Command Execution](#)

–

[Parallels Desktop Flaw Lets Non-Admin Mac Users Gain Root, but Intel Macs Can't Install Fix](#)

–

[Google Patches Pixel Modem Flaw Amid Signs of Limited Targeted Exploitation](#)

–

[Acronis cPanel Backup Plugin Vulnerability Exploited in Targeted Attacks](#)

[Read more >](#)

The News

Top of the news



China-Linked Hackers Exploit Chrome-Windows Zero-Day Chain to Deploy GRIMWEDGE

A Chinese threat actor has been attributed to a spear-phishing campaign that exploits recently patched security flaws in Google Chrome and Microsoft Windows to deliver a malicious JavaScript backdoor called GRIMWEDGE.

Volexity, which is tracking the threat cluster under the moniker UTA0560, said the activity targeted multiple non-governmental organizations (NGOs) on September 1, 2026.

"The emails contained a message encouraging the users to click a link that led to the website of a U.S.-based university," researchers Ankur Saini, Conor Quigley, Sean Koessel, Steven Adair, and Tom Lancaster said. "These links abused a reflected cross-site scripting (XSS) vulnerability on the website, redirecting recipients to threat-actor-controlled infrastructure hosting a multi-stage exploit chain." The exploit chain, as previously highlighted by Proofpoint, involves three separate flaws – two in Chrome and one in Windows Advanced Local Procedure Call (ALPC). It first abuses CVE-2026-85046 to gain arbitrary read/write within the V8 sandbox, then escapes the browser sandbox via CVE-2026-87491, and finally employs CVE-2026-85880 to inject code into the Chrome browser process and achieve arbitrary code execution.

[Read more >](#)

Other news highlights

[Cisco Secure Email Gateway Flaw Exploited in the Wild, Enables Root Command Execution](#)

[New DDRop Attack Breaks Intel TDX and AMD SEV-SNP Confidential Computing](#)

[Telegram Desktop Flaw Lets Hidden JavaScript Exfiltrate Messages From HTML Exports](#)

[WordPress Adds Automated Plugin Reviews to Block High-Risk Updates Before Distribution](#)

Geo-Politics

News from around the world



Other news highlights

[KREMLIN Banking Malware Hijacks Chrome and Edge to Steal Credentials and Session Tokens](#)

[U.S. Seizes NightmareStresser Domains Linked to Hundreds of Thousands of DDoS Attacks](#)

[Russian State-Sponsored Hackers Use Claude to Rebuild Malware After Detection](#)

[Three Threat Groups Target Russian Enterprises With Backdoors, Ransomware, and Wipers](#)

Iranian Hackers Use Telegram-Controlled Malware to Spy on Dissidents and Journalists

Cybersecurity agencies in the United States, the United Kingdom, and the Netherlands have detailed a Windows malware that they say Iran's intelligence service uses to spy on dissidents, journalists, and activists around the world.

The malware is controlled via the Telegram messaging app and can copy a target's emails and chat messages, take screenshots, and activate the microphone to record audio.

The FBI calls it HEAVYGRAM, and the U.K.'s National Cyber Security Center (NCSC) calls it CHOSEN BRICK.

The joint advisory was published on September 15 by the NCSC, the FBI, and the Netherlands' intelligence service, the AIVD.

The FBI also released an updated analysis of the malware that expands on a March 2026 alert, the first to describe the campaign, with more technical detail and new indicators of compromise.

The FBI attributes the malware to Iran's Ministry of Intelligence and Security (MOIS), the country's main intelligence agency, and dates the wider campaign to the autumn of 2023. The advisory says CHOSEN BRICK has been used against people in the U.K., the U.S., and the Netherlands, and around the world, since at least 2025.

[Read more >](#)

Breaches

Security Breaches this week



Personal, Financial Info Exposed in Revolut Data Breach

British fintech giant Revolut is notifying a subset of users that their personal and financial information was compromised in a data breach.

Based in London, the neobank and financial technology company provides banking and investment services to over 80 million users in 160 countries and regions.

Late last week, the company informed a small number of users that their personally identifiable information (PII) was exposed to a third party posing as a government agency.

The exposed data, it said in emails to the affected users, included names, addresses, phone numbers, email addresses, dates of birth, occupation, copies of driver's licenses and passports, and verification selfies.

Financial information, including IBANs, account statements, withdrawal records, and full transaction history, including Bitcoin, was also exposed.

The request carried valid technical domain credentials and was treated as an authentic agency inquiry. All financial institutions must comply with legal requests from law enforcement and government agencies.

[Read more >](#)

Other news highlights

[280,000 Impacted by Premier Medical Group Data Breach](#)

[Texas Utility CenterPoint Energy Confirms Breach After Hacker Leaks Data](#)

[240,000 Hit by Data Breach at Japan's Digital Agency](#)

[First Agentic AI Data Breach Reported to Spanish Regulator](#)

Vulnerabilities

Vulnerabilities & Exploits



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 score: 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 score: 8.8

Last weeks recaps

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 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 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 9.8

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



NOva Phishkit Targets US and EU Businesses: A New Challenge for Identity Security

NOva is targeting organizations across North America and Europe with phishing campaigns that impersonate trusted services and abuse legitimate authentication flows. Successful attacks can give threat actors access to valid accounts without relying on obvious malware activity.

From there, a single compromised identity can open the door to sensitive data, business systems, and additional cloud resources.

The longer that access goes unnoticed, the greater the potential for wider compromise, operational disruption, and financial loss. NOva activity has been observed across organizations in government, technology, consulting, healthcare, and other sectors in North America and Europe. Its use of trusted business platforms and cloud services makes the campaign relevant across a wide range of organizations.

[Read more >](#)

Other news highlights

[Attackers Use Passkey Phishing to Hijack Microsoft Cloud Accounts and Exfiltrate Data](#)

[Claude Used to Automate Exploitation and Data Theft Across Multiple Victims](#)

[NTrezor: 347,000 users targeted in phishing attacks after Brevo breach](#)

[Threat Actor Generates 1M Personalized Fraud Emails in 3 Days](#)