SCC | DIGITAL

THREAT PULSE

Amateurs hack systems;
professionals hack people
- Bruce Schneier

THREATS

NEWS

PHISHING

February 2026 - VOL.4

The News

IN THE NEWS THIS WEEK

Cisco SD-WAN Zero-Day CVE-2026-20127 Exploited Since 2023 for Admin Access

A newly disclosed maximum-severity security flaw in Cisco Catalyst SD-WAN Controller (formerly vSmart) and Catalyst SD-WAN Manager (formerly vManage) has come under active exploitation in the wild as part of malicious activity that dates back to 2023.

The vulnerability, tracked as CVE-2026-20127 (CVSS score: 10.0), allows an unauthenticated remote attacker to bypass authentication and obtain administrative privileges on the affected system by sending a crafted request to an affected system.

Successful exploitation of the flaw could allow the adversary to obtain elevated privileges on the system as an internal, high-privileged, non-root user account.

"This vulnerability exists because the peering authentication mechanism in an affected system is not working properly," Cisco said in an advisory, adding the threat actor could leverage the non-root user account to access NETCONF and manipulate network configuration for the SD-WAN fabric.

READ MORE

OTHER NEWS HIGHLIGHTS

Malicious NuGet Packages Stole ASP.NET Data; npm Package Dropped Malware

SolarWinds Patches 4 Critical Serv-U 15.5 Flaws Allowing Root Code Execution

CISA Confirms Active Exploitation of FileZen CVE-2026-25108 Vulnerability

The News

TOP OF THE NEWS THIS WEEK

SolarWinds Patches Four Critical Serv-U Vulnerabilities

SolarWinds on Tuesday announced patches for four critical-severity vulnerabilities in its enterprise file transfer solution, Serv-U.

All four security defects, tracked as CVE-2025-40538 to CVE-2025-40541, have a CVSS score of 9.1, could result in remote code execution, and impact Serv-U version 15.5.

CVE-2025-40538, SolarWinds explains, is a broken access control issue that could allow threat actors to create a system admin user and execute arbitrary code with the elevated privileges of domain admin or group admin.

CVE-2025-40539 and CVE-2025-40540 are type confusion flaws that allow attackers to execute code with elevated privileges, the company notes, without providing additional details.

CVE-2025-40541 is described as an insecure direct object reference (IDOR) bug leading to the execution of native code in the context of a privileged account.

The successful exploitation of all four vulnerabilities, SolarWinds explains, requires that an attacker have administrative privileges on the vulnerable Serv-U instance.

READ MORE

TOP RELATED ARTICLES

Trend Micro Patches Critical Apex One Vulnerabilities

RoguePilot Flaw in GitHub Codespaces Enabled Copilot to Leak GITHUB_TOKEN

Claude's New AI Vulnerability Scanner Sends Cybersecurity Shares Plunging

Geo-Politics

NEWS FROM AROUND THE WORLD

Defense Contractor Employee Jailed for Selling 8 Zero-Days to Russian Broker

A 39-year-old Australian national who was previously employed at U.S. defense contractor L3Harris has been sentenced to a little over seven years in prison for selling eight zero-day exploits to Russian exploit broker Operation Zero in exchange for millions of dollars.

Peter Williams pleaded guilty to two counts of theft of trade secrets in October 2025. In addition to the jail term, Williams has been ordered to serve three years of supervised release with special conditions, as well as forfeit illicit proceeds, including properties, clothing, jewelry, and luxury watches, purchased from the cryptocurrency payments he received in return for selling the exploits.

The case's connection to Operation Zero was disclosed by cybersecurity journalist Kim Zetter late last year. The nature of the exploits are presently unclear. But a sentencing memorandum published earlier this month revealed that the tools could have been "used against any manner of victim, civilian or military around the world, and engage in all manner of crime from cyber fraud, theft, and ransomware, to state directed spying and offensive cyber operations against military targets."

READ MORE

HIGHLIGHTS FROM AROUND THE WORLD

Breaches

SECURITY BREACHES THIS WEEK

CarGurus Data Breach Impacts Over 12 Million Users

More than 12 million users have been affected by a data breach at automotive research and shopping website CarGurus.

The incident was disclosed last week, when the infamous extortion group ShinyHunters added CarGurus to its Tor-based leak site, claiming the theft of personally identifiable information (PII) and internal corporate data.

Initially, the hackers said they stole 1.7 million records from the company, but have since leaked a 6.1GB archive that contains information pertaining to approximately 12.5 million accounts.

The compromised information, data breach notification website Have I Been Pwned says, includes names, addresses, email addresses, phone numbers, and IP addresses.

“Following an attempted extortion, the data was published publicly and contained more than 12M email addresses across multiple files, including user account ID mappings, finance pre-qualification application data, and dealer account and subscription information,” the breach notification service says.

In a post on X, Have I Been Pwned noted that roughly 70% of the email addresses in the data set have been compromised in other data breaches as well and were already in its database.

READ MORE

OTHER SECURITY BREACHES

Apex Spine & Neurosurgery Data Breach Investigation

Japanese chip-testing toolmaker Advantest suffers ransomware attack

Meta Files Lawsuits Against Brazil, China, Vietnam Advertisers Over Celeb-Bait Scams

Vulnerabilities

VULNERABILITIES & EXPLOITS

CVE-2026-20127 Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability

CVSS SCORE 10.0

CVE-2026-3061: Out of bounds read in Google Chrome

CVSS SCORE 9.1

LAST WEEKS RECAP

CVE-2026-26119 Privilege Escalation in Windows Admin Center
CVSS Score: (8.8)

CVE-2026-22769 Dell RecoverPoint for Virtual Machines (RP4VMs) Use of Hard-coded Credentials Vulnerability
CVSS Score: (10.0)

Ransomware

WEEKLY RANSOMWARE ROUNDUPS

OVERVIEW

A total of 138 new victims were reported across various ransomware groups this Week.

TARGET INDUSTRIES

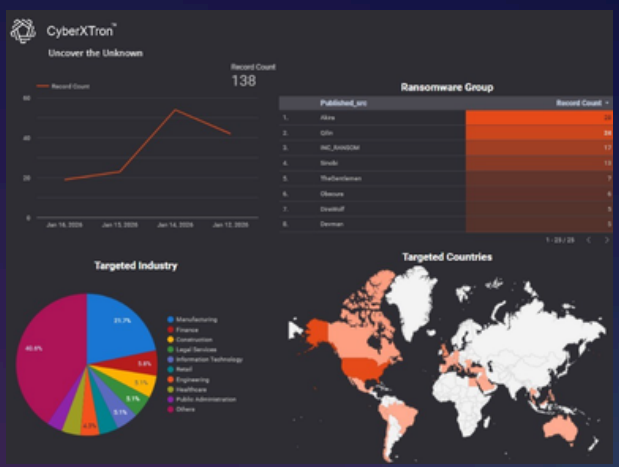
The Manufacturing sector was the primary focus, representing 21.7% of all victims.

TARGET COUNTRY

The USA was the top victim country, with a total of 76 affected entities.

TOP GROUP

The Akira was the most active, claiming 28 victims.



Dive into this interactive report to uncover hidden trends HERE!

Published Ransomware Attacks - Source: CyberXTron ThreatBolt

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.

Akira

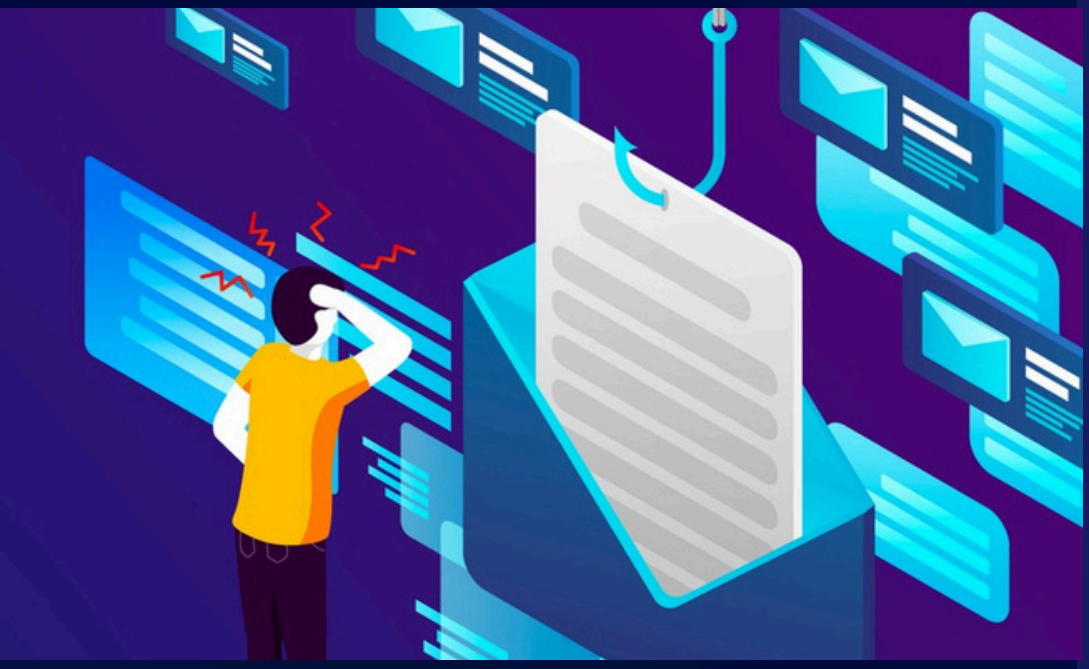
Akira is a ransomware strain that appeared in March 2023, targeting over 250 organisations including BHI Energy, Nissan Australia, Tietoevry, and Stanford University. Operating as ransomware-as-a-service, it earned up to $42 million by April 2024.

Clop

Clop ransomware first emerged in 2019, when it became a prevalent threat to organizations and businesses. Clop ransomware encrypts the victims files and threatens to leak the confidential information if no ransom is paid.

Phishing

PHISHING NEWS THIS WEEK



Phishing campaign targets freight and logistics orgs in the US, Europe

A financially motivated threat group dubbed “Diesel Vortex” is stealing credentials from freight and logistics operators in the U.S. and Europe in phishing attacks using 52 domains.
In a campaign that has been running since September 2025, the threat actor has stolen 1,649 unique credentials from platforms and service providers critical in the freight industry.
Some of the Diesel Vortex victims include DAT Truckstop, TIMOCOM, Teleroute, Penske Logistics, Girteka, and Electronic Funds Source (EFS). Researchers at the typosquatting monitoring platform Have I Been Squatted uncovered the campaign after finding an exposed repository containing an SQL database from a phishing project that the threat actor called Global Profit and marketed it to other cybercriminals under the name MC Profit Always.
The repository also included a file with Telegram webhook logs that revealed communications between the phishing service operators. Based on the language used, the researchers believe that Diesel Vortex is an Armenian-speaking actor connected to Russian infrastructure.

READ MORE

OTHER PHISHING ARTICLES

Microsoft Warns Developers of Fake Next.js Job Repos Delivering In-Memory Malware

Google Disrupts UNC2814 GRIDTIDE Campaign After 53 Breaches Across 42 Countries

MuddyWater Targets MENA Organizations with GhostFetch, CHAR, and HTTP_VIP