Simplify the complex

Threat Pulse

Threats • News • Phishing

Amateurs hack systems; professionals hack people

– Bruce Schneier

SCC Threat Pulse | OCT | Vol.1

The News



Cisco SD-WAN zero-day gives unauthenticated attackers admin access

Cisco disclosed CVE-2026-76504 on 30 September and confirmed active exploitation of a critical authentication bypass in Catalyst SD-WAN Manager. A remote attacker without credentials can send a crafted HTTP request and gain API access with administrator privileges. Cisco rates it CVSS 9.8.

The affected component is the central management plane for Cisco SD-WAN deployments. Compromise could expose network configuration and provide control over managed infrastructure, making this relevant to transport, engineering, construction, government and organizations with distributed sites. Cisco lists fixed releases and says there is no workaround. Internet-exposed managers are at elevated risk; Cisco's advisory includes indicators involving encoded requests to the login endpoint and identifies log files to review. Defender focus: identify every Catalyst SD-WAN Manager, upgrade to a fixed release, restrict management access to trusted networks, and review Cisco's specified logs for suspicious requests. If indicators are present, collect admin-tech files and contact Cisco TAC.

Read more ›

Other news highlights

Roundcube webmail SQL injection exploited

–

CISA flags exploited WSO2 and Adobe flaws

–

Bank supplier breach exposes customer records

–

UK universities face rising web attacks

The News

Top of the news



OpenSSL patches a DTLS flaw that can leak heap memory or crash services

OpenSSL's 29 September security update fixedCVE-2026-84782, a high-severity bug in DTLS retransmission handling. Under specific conditions, a peer may receive heap memory as plaintext handshake data; a read from an unmapped region can instead crash the process.

The issue affects products using vulnerable OpenSSL branches when they expose a DTLS endpoint. DTLS is used over UDP in some real-time, VPN, and other latency-sensitive services, but exposure depends on how each product uses the library.

OpenSSL also described memory-consumption and denial-of-service issues in the release. The advisories reviewed for this brief did not report in-the-wild exploitation of CVE-2026-84782 as of 1 October.

Check vendor advisories and software inventories for bundled OpenSSL versions, then update through supported package channels. Where immediate updates are not possible, identify internet-reachable DTLS services and apply vendor-approved exposure controls while remediation is tracked.

Read more ›

Other news highlights

Kiteworks restores systems after critical flaw

–

FBI declares incident after employee data theft

–

Keio railway disrupted by ransomware

–

Times Car confirms 6.6 million accounts exposed

Geo-Politics



Zero-day breach exposes Belnet email infrastructure to data theft

Belgian research and education network Belnet disclosed a security incident on 25 September after identifying a zero-day vulnerability in a supplier's technology. Attackers copied incoming emails sent to Belnet and one customer between 22 July and the morning of 25 September to external infrastructure.

Belnet said it remediated the vulnerability by 25 September at 08:10 and engaged Belgium's Centre for Cybersecurity for incident response and forensics. A 29 September update said the exploited flaw was fixed and the incident was under control, while the investigation continued.

The event matters to public services, universities, research institutions and organizations that rely on shared network and messaging infrastructure. The supplier has not been named in the public notice, and the final scope remains under investigation.

Defender focus: establish whether staff or business units exchanged email with Belnet during the exposure window, follow Belnet's direct notice, review related attachments or credentials, and treat the initial impact scope as provisional pending forensic findings.

Read more ›

Other news highlights

CISA warns of RouterOS pre-authentication RCE

–

Mozilla patches high-impact Firefox flaws

–

ShinyHunters resume Oracle PeopleSoft attacks

–

Researchers find 543,000 valid leaked credentials

Breaches

Security Breaches this week



Bitget reports a $351.6m theft; North Korea link remains provisional

Cryptocurrency exchange Bitget said its systemsdetected unauthorized transfers from a small number of hot wallets on 24 September. The Hacker News reported the loss at about $351.6 million across several digital assets and blockchains. Bitget said cold wallets were unaffected and trading and deposits remained operational.

Bitget CEO Gracy Chen said the activity was highly consistent with known North Korean threat actor patterns, based on IP behavior and on-chain analysis. The company has not published the underlying evidence or named a group, so this remains an attribution assessment.

Bitget said an attacker abused a critical backend system in its wallet infrastructure to approve fraudulent transfers. Mandiant and SlowMist are assisting with the investigation; some associated wallet addresses have reportedly been frozen.

Response focus for digital-asset operators: review signing and transaction-approval workflows, separate hot-wallet administration from production services, and preserve access records for the incident window. Do not treat a reported attribution as proof of the initial access method.

Read more ›

Other news highlights

Cloudflare fixes cross-tenant data exposure

–

TeamViewer urges urgent patching of severe flaws

–

Spectre variant leaks Linux root password hashes

–

Misconfigured Supabase databases expose credentials

Vulnerabilities

Vulnerabilities & Exploits



CVE-2026-87902 | WordPress Core path traversal can include a readable local PHP file and, under server/theme preconditions, lead to remote code execution. CISA added it to KEV on 25 September after exploitation evidence. CVSS 8.1.

CVSS score: 8.1

CVE-2026-94127 | F5 BIG-IP APM heap overflow may permit unauthenticated remote code execution when an APM access policy and OAuth profile share a virtual server. F5 reports active exploitation. CVSS 9.8 (v3.1); 9.3 (v4).

CVSS score: 9.8

NEW THIS WEEK (24-30 SEP): CVE-2026-76504 - Cisco Catalyst SD-WAN Manager auth bypass, CVSS 9.8; exploitation confirmed. CVE-2026-65660 - SharePoint code injection, CVSS 8.8; exploitation observed. CVE-2026-88771/-88772 - Citrix NetScaler, CVSS 9.5 each; active exploitation. CVE-2026-84782 - OpenSSL DTLS memory disclosure/crash; fixes issued 29 September. Patch Cisco, Microsoft and Citrix systems; inventory bundled OpenSSL.

Last weeks recaps

CVE-2026-76460 - Cisco ISE
CVSS 10.0. Unauthenticated API authentication bypass; Cisco confirms active exploitation. Apply the fixed ISE release; no workaround is available.

CVE-2026-58704 - Google Pixel modem
CVSS 8.8. Permission-bypass flaw may allow nearby privilege escalation without user interaction. Google reports limited, targeted exploitation; install the September security update.

CVE-2026-76504 - Cisco SD-WAN
CVSS 9.8. Unauthenticated API access can grant administrator privileges. Cisco confirms active exploitation; upgrade and restrict management interfaces.

CVE-2026-65660 - Microsoft SharePoint
CVSS 8.8. Authenticated code injection with active exploitation reported. Apply supported SharePoint fixes and verify exposed on-premises servers.

Ransomware

Weekly Ransomware Roundups



Overview

CyberXTron's September posts profile a broad extortion picture. EndZone's leak site lists five victim claims and Cinder claims eight organizations; these are operator or tracker claims, not confirmed incident totals.

Target industries

Monthly posts span professional services, telecommunications, technology, government-facing software, manufacturing, education, finance, retail, and healthcare.

Target country

CyberXTron's September cases include claimed victims in the United States, United Kingdom, Italy, and countries across Asia and Europe. Independently verify any exposed organization before escalation.

Top Group

CyberXTron reports 17-18 Silent Ransom Group listings in each of August and September. The group is described as using social engineering and remote-access tools for data theft without encrypting files.

Top Threat Actors

EndZone

Five victim claims since 18 September. The group claims data theft and disruption; CyberXTron says its technical and impact claims are not independently verified.

–

Cinder

Eight U.S. organizations and about 12.3 TiB are claimed. CyberXTron found no public evidence of encryption; treat the listings as extortion claims.

–

Silent Ransom Group

CyberXTron describes an extortion-only operation using social engineering and legitimate remote-access tools. Its site showed 17-18 listings in each of August and September.

Phishing

Phishing news this week



CSuite phishing steals Microsoft 365 sessions and installs remote-access tools

A 30 September investigation from ANY.RUN found CSuite phishing lures impersonating common business services, including Microsoft 365 and Adobe. The campaign combines account/session theft with installation of legitimate remote-management tools such as ScreenConnect or Action1.

Researchers observed the campaign across 351 sandbox analyses. Technology, manufacturing, government and consulting were among the most exposed sectors; lures also included a forged DocuSign envelope styled as a law-firm communication.

The chain can give an attacker access to both a Microsoft 365 account and an employee endpoint, supporting mailbox surveillance, payment fraud and persistent remote access. These are conventional phishing and remote-access techniques, rather than AI-generated attacks.

Defender focus: review Microsoft 365 sign-ins and session revocation, block unauthorized RMM deployments, monitor new remote-access services and suspicious script execution, and independently verify payment, NDA and file-sharing requests.

Read more ›

Other news highlights

Apple fixes exploited CoreGraphics zero-day

–

Microsoft hardens Entra ID against script injection

Russian state hackers deploy malware via RedFlick

–

Former Air Force members sentenced over BEC scams