Crowe

Weekly Cyber Security Bulletin

Threat Advisory & Security News

4 - 10 May 2026

Audit/Tax/Consulting

Smart decions. Lasting value.

1. Summary

Vulnerability Details

- Palo Alto Networks PAN-OS Zero-Day Vulnerability Exploited in Active Attacks (CVE-2026-0300)
- Multiple Cisco Enterprise Product Vulnerabilities Enabling SSRF, Code Execution, and Denial-of-Service Attacks (CVE-2026-20034, CVE-2026-20035, CVE-2026-20185, CVE-2026-20188, CVE-2026-20167)
- Critical Android Remote Code Execution Vulnerability in ADB Daemon (CVE-2026-0073)

Attack Campaigns

- NVIDIA GeForce NOW Service Provider Data Breach Exposes User Information
- Trellix Confirms Source Code Repository Breach

Security News

- Microsoft Warns of Large-Scale AiTM Phishing Campaign Targeting 35,000 Users
- AI-Assisted Intrusion Targeted Mexican Water Utility OT Environment
- Hackers Use Fake Claude AI Installer Pages to Deliver Malware

2. Vulnerability Details

2.1 Palo Alto Networks PAN-OS Zero-Day Vulnerability Exploited in Active Attacks (CVE-2026-0300)

Release Date – 7 May 2026

CVE Details – CVE-2026-0300

CVSS Score – 9.3 (Critical)

Affected Product – Palo Alto Networks PAN-OS (PA-Series and VM-Series Firewalls)

Description –

Palo Alto Networks has disclosed a critical zero-day vulnerability in PAN-OS that allows unauthenticated remote attackers to execute arbitrary code with root privileges on affected firewall devices.

The vulnerability exists in the User-ID Authentication Portal (Captive Portal) service due to an out-of-bounds write weakness (CWE-787) that can be triggered through specially crafted network packets.

According to Palo Alto Networks, limited exploitation activity has already been observed in the wild targeting internet-exposed User-ID Authentication Portals.
The issue specifically impacts PA-Series and VM-Series firewalls configured with:

- User-ID Authentication Portal enabled
- Interface Management Profiles exposing response pages to untrusted or internet-facing networks
-

Prisma Access, Cloud NGFW, and Panorama appliances are not affected by this vulnerability.
The vulnerability affects multiple PAN-OS versions across 10.2, 11.1, 11.2, and 12.1 branches. Palo Alto Networks has announced patched releases with staged availability dates beginning May 13, 2026, and May 28, 2026.

Palo Alto Networks has also released Threat Prevention signatures capable of detecting and blocking exploitation attempts through Threat ID 510019.

Mitigation and Recommendations –

Organizations using affected Palo Alto Networks firewalls should immediately apply mitigation measures and prioritize emergency patch deployment once fixes become available.
Recommended actions include:

- Restricting User-ID Authentication Portal access to trusted internal IP addresses only
- Disabling Response Pages on interfaces exposed to untrusted or internet-facing networks
- Disabling the User-ID Authentication Portal entirely if not operationally required
- Enabling Threat Prevention signature Threat ID 510019 with updated Applications and Threats content
- Monitoring firewall logs for suspicious authentication portal activity or exploitation attempts
- Reviewing internet-exposed firewall interfaces and management profiles Applying PAN-OS updates immediately upon vendor release availability

Given the confirmed active exploitation and root-level remote code execution impact, organizations should treat this vulnerability as a highest-priority security threat.

Reference: https://security.paloaltonetworks.com/CVE-2026-0300

2.2 Multiple Cisco Enterprise Product Vulnerabilities Enabling SSRF, Code Execution, and Denial-of-Service Attacks (CVE-2026-20034, CVE-2026-20035, CVE-2026-20185, CVE-2026-20188, CVE-2026-20167)

Release Date – 6 May 2026
CVE Details –
CVE-2026-20034, CVE-2026-20035, CVE-2026-20185, CVE-2026-20188, CVE-2026-20167
CVSS Score –
CVE-2026-20034 – 8.8 (High), CVE-2026-20035 – 8.8 (High), CVE-2026-20185 – 7.7 (High), CVE-2026-20188 – 7.5 (High), CVE-2026-20167 – 7.7 (High)
Affected Products – Cisco Unity Connection, SG350/SG350X Switches, Crosswork Network Controller (CNC), Network Services Orchestrator (NSO), IoT Field Network Director

Description –

Cisco has released security updates addressing multiple high-severity vulnerabilities affecting several enterprise networking and infrastructure products.

Two vulnerabilities, tracked as CVE-2026-20034 and CVE-2026-20035, impact Cisco Unity Connection and could allow authenticated remote attackers to perform server-side request forgery (SSRF) attacks or execute arbitrary code with root privileges.

The flaws are caused by insufficient validation of user-supplied input and specially crafted HTTP requests. Successful exploitation could enable attackers to send unauthorized network requests originating from the affected device or gain elevated system-level access.

Cisco also addressed CVE-2026-20185, a high-severity denial-of-service vulnerability affecting the SNMP subsystem of Cisco SG350 and SG350X switches. The vulnerability results from improper error handling during parsing of SNMP response data. Attackers possessing valid SNMP credentials or community strings could exploit the flaw to force affected devices to reload unexpectedly, leading to service disruption.

Another high-severity vulnerability, CVE-2026-20188, affects Cisco Crosswork Network Controller (CNC) and Network Services Orchestrator (NSO). Due to improper implementation of connection rate limiting, unauthenticated remote attackers can exhaust system resources by sending large volumes of connection requests, causing denial-of-service conditions.

Additionally, Cisco patched CVE-2026-20167 in the web interface of IoT Field Network Director. The flaw is caused by improper error handling and could allow attackers to submit crafted input that forces the affected router to reload, resulting in denial-of-service conditions.

Cisco also resolved several medium-severity vulnerabilities affecting additional enterprise products, including Identity Services Engine (ISE), Slido, Prime Infrastructure, and Enterprise Chat and Email (ECE). These vulnerabilities could enable command execution, information disclosure, file access, arbitrary log downloads, and browser-based attacks.

At the time of disclosure, Cisco stated that there is no evidence of active exploitation of these vulnerabilities in the wild.

Mitigation and Recommendations –

Organizations should immediately apply the latest Cisco security updates and firmware patches for all affected products.

Additional recommended actions include:

- Updating affected Cisco enterprise products to the latest supported versions
- Restricting access to management interfaces and administrative services
- Limiting SNMP exposure and enforcing strong SNMP credentials
- Implementing network segmentation for critical infrastructure devices
- Monitoring systems for abnormal connection requests or device reload events
- Reviewing logs for suspicious administrative or HTTP activity
- Disabling unnecessary externally exposed services wherever possible

Given the enterprise impact and potential for code execution, SSRF exploitation, and denial-of-service attacks, organizations should prioritize remediation efforts across all affected Cisco deployments.

Reference: https://sec.cloudapps.cisco.com/security/center/publicationListing.x

2.3 Critical Android Remote Code Execution Vulnerability in ADB Daemon (CVE-2026-0073)

Release Date – 4 May 2026
CVE Details – CVE-2026-0073
CVSS Score – 8.8 (High)
Affected Product – Android System Component (adbd / Android Debug Bridge daemon)

Description –

Google has released security updates to address a high-severity vulnerability affecting the Android System component.

The vulnerability, tracked as CVE-2026-0073, exists within the adbd_tls_verify_cert function of Android's auth.cpp component and is caused by a logic error in the wireless Android Debug Bridge (ADB) mutual authentication process.

Successful exploitation allows a remote proximal or adjacent attacker to bypass wireless ADB authentication mechanisms and execute arbitrary code as the shell user without requiring additional execution privileges or any user interaction.

The issue specifically impacts the Android Debug Bridge daemon (adbd), which manages communication between Android devices and connected systems for debugging and shell access operations. Due to improper certificate verification during wireless ADB authentication, attackers located on the same or nearby network could potentially compromise vulnerable Android devices remotely.

Although the vulnerability does not directly provide full root privileges, execution as the shell user may still enable attackers to perform sensitive operations, manipulate device configurations, access debugging interfaces, and potentially chain the flaw with additional vulnerabilities for deeper system compromise.

At the time of disclosure, Google stated that there is no evidence of active exploitation in the wild. However, due to the low attack complexity, lack of user interaction requirements, and remote attack vector, the vulnerability poses a significant security risk for enterprise and consumer Android environments.

Mitigation and Recommendations –

Organizations and users should immediately apply the latest Android security updates released by Google.

Additional recommended actions include:

- Applying the May 2026 Android security patches immediately
- Disabling wireless ADB functionality where not operationally required
- Restricting developer options and debugging features on production devices
- Enforcing Mobile Device Management (MDM) policies across enterprise devices
- Monitoring devices for suspicious shell activity or unauthorized debugging sessions
- Ensuring devices are connected only to trusted networks

Given the potential for remote code execution without user interaction, organizations should prioritize patch deployment across all affected Android devices and environments.

Reference:

- https://source.android.com/docs/security/bulletin/2026/2026-05-01

3. Attack Campaigns

3.1 NVIDIA GeForce NOW Service Provider Data Breach Exposes User Information

Description –

GFN CLOUD INTERNET SERVICES, operating the GFN.AM cloud gaming platform for NVIDIA GeForce NOW services, has disclosed a data breach involving unauthorized access to its backend database.

According to the company, the unauthorized access occurred on March 9, 2026, but was only detected on May 2, 2026, resulting in an exposure window of approximately 54 days before discovery and containment.

The breach affects users registered on the GFN.AM platform on or before March 9, 2026. Accounts created after that date were reportedly not impacted.

The company confirmed that threat actors gained access to sensitive user information stored within the platform database. Exposed data may include:

- Email addresses
- Phone numbers associated with mobile operator registrations
- Dates of birth
- Full names for users authenticated through Google Sign-In
- GFN.AM usernames

GFN.AM stated that account passwords were not compromised during the incident. However, the exposed personal information significantly increases the risk of phishing attacks, social engineering campaigns, SIM-swapping attempts, and credential-stuffing attacks targeting affected individuals.

Following discovery of the breach, the company stated that it implemented additional technical and organizational security controls to secure its infrastructure and remediate the unauthorized access.

At the time of disclosure, the organization had not publicly confirmed the exact attack vector, whether the breach resulted from stolen credentials, software vulnerabilities, or database misconfigurations.

Mitigation and Recommendations –

Users affected by the GFN.AM data breach should immediately take precautionary security measures to reduce the risk of account compromise and targeted phishing attacks.
Recommended actions include:

- Monitoring email accounts for suspicious login attempts and phishing messages
- Being cautious of unsolicited phone calls, SMS messages, or emails referencing GFN.AM or NVIDIA services
- Enabling multi-factor authentication (MFA) on email and linked Google accounts
- Reviewing Google account activity and connected sessions for suspicious behavior
- Resetting passwords on accounts that reuse similar credentials
- Monitoring financial and telecom accounts for signs of fraud or SIM-swapping attempts
- Avoiding interaction with unexpected links or attachments claiming to relate to the breach

Organizations should continue monitoring for follow-up phishing campaigns leveraging the exposed user information from this incident.

Reference:
https://gfn.am/hy/blog/%D5%A1%D5%B6%D5%BE%D5%BF%D5%A1%D5%B6%D5%A3%D5%B8%D6%82%D5%A9%D5%B5%D5%A1%D5%B6-%D5%B4%D5%AB%D5%BB%D5%A1%D5%A4%D5%A5%D5%BA/

3.2 Trellix Confirms Source Code Repository Breach

Description –

Cybersecurity company Trellix has confirmed that a portion of its source code repository was compromised following a recent security incident.

The company stated that it is actively investigating the intrusion with assistance from forensic experts and has also notified law enforcement authorities regarding the breach.

According to Trellix, there is currently no evidence indicating that its source code release or software distribution processes were affected. The company also stated that it has not identified any signs of malicious exploitation involving the exposed source code.

At the time of disclosure, Trellix had not publicly confirmed the exact intrusion timeline, the threat actor responsible, or the specific products and repositories impacted during the compromise.

The incident is suspected to be potentially linked to the broader software supply chain attack campaign associated with the TeamPCP and Lapsus$ threat groups. This campaign previously targeted multiple cybersecurity and software organizations, including Checkmarx, Aqua Security, and Bitwarden.

The broader campaign involved compromises of CI/CD pipelines, trojanized software components, malicious extensions, and credential theft operations designed to exfiltrate sensitive source code and enterprise secrets from affected organizations.

Mitigation and Recommendations –

Organizations using Trellix products should continue monitoring for official security updates and advisories from the vendor.

Recommended actions include:

- Monitoring vendor advisories for additional indicators of compromise or affected product disclosures
- Reviewing software integrity validation processes for third-party security tools
- Monitoring CI/CD environments and software repositories for unauthorized modifications
- Enforcing strong credential protection and MFA across development environments
- Conducting threat hunting activities for signs of supply chain compromise
- Validating hashes and signatures of downloaded software packages and updates
- Restricting privileged access to source code repositories and developer environments

Organizations should remain vigilant as supply chain attacks targeting software vendors and cybersecurity providers continue to increase in sophistication and impact.

Reference: https://www.trellix.com/statement/

4. Security News

4.1 Microsoft Warns of Large-Scale AiTM Phishing Campaign Targeting 35,000 Users

Description –

Microsoft has disclosed details of a large-scale credential theft campaign targeting more than 35,000 users across over 13,000 organizations in 26 countries between April 14 and April 16, 2026.

According to Microsoft Threat Intelligence, approximately 92% of the targeted users were located in the United States, with healthcare and life sciences, financial services, professional services, and technology sectors among the most heavily targeted industries.

The phishing campaign used enterprise-style HTML email templates impersonating internal compliance and regulatory communications. Attackers used display names such as “Internal Regulatory COC,” “Workforce Communications,” and “Team Conduct Report” to increase legitimacy.

The phishing emails contained urgent subject lines related to alleged conduct policy violations and non-compliance investigations designed to pressure users into immediate action. The emails were reportedly sent using legitimate email delivery services, helping them bypass traditional email filtering protections.

Victims received PDF attachments containing malicious links that redirected them through multiple CAPTCHA verification stages before reaching adversary-in-the-middle (AiTM) phishing pages engineered to harvest Microsoft credentials and authentication tokens in real time. This allowed attackers to bypass multi-factor authentication (MFA) protections and gain unauthorized account access.

Microsoft additionally reported a major rise in QR code phishing attacks during Q1 2026, with attack volumes increasing by 146%, from 7.6 million attacks in January to 18.7 million in March. The company also observed continued activity linked to phishing-as-a-service (PhaaS) platforms including Tycoon 2FA, Kratos, and EvilTokens.

Reference: https://www.microsoft.com/en-us/security/blog/2026/05/04/breaking-the-code-multi-stage-code-of-conduct-phishing-campaign-leads-to-aitm-token-compromise/

4.2 AI-Assisted Intrusion Targeted Mexican Water Utility OT Environment

Description –

Dragos has disclosed details of a cyber intrusion targeting a municipal water and drainage utility in Monterrey, Mexico, where threat actors extensively leveraged AI models including Claude and GPT to assist attack operations.

According to Dragos, the intrusion occurred in January 2026 as part of a broader campaign targeting multiple Mexican government organizations between December 2025 and February 2026. The activity is currently tracked as TAT26-12.

Researchers stated that the attackers used Anthropic's Claude model as the primary operational engine for intrusion planning, offensive tool development, privilege escalation guidance, and reconnaissance activities, while OpenAI GPT models were reportedly used for victim data processing and structured reporting.

One of the most significant findings was a 17,000-line Python offensive framework generated and iteratively refined by Claude during the intrusion. The framework reportedly included 49 modules covering credential harvesting, Active Directory reconnaissance, database access, and privilege escalation techniques.

During internal reconnaissance activities, Claude independently identified a vNode SCADA and IIoT management interface within the targeted environment and classified it as a high-value operational technology (OT) asset associated with critical infrastructure.

Researchers emphasized that the attackers did not explicitly instruct the AI to search for OT systems. Instead, the AI autonomously identified the industrial platform during broader network reconnaissance and recommended it as a priority target.

Claude subsequently analyzed the platform, identified its single-password authentication mechanism, researched publicly available vendor documentation, assembled credential lists, and recommended password-spraying attacks against the interface.

Although the attempted attacks against the OT environment were unsuccessful and no industrial control systems were compromised, Dragos warned that the incident demonstrates how AI tools can significantly accelerate offensive cyber operations and increase the visibility of operational technology environments to attackers with limited ICS expertise.

The threat actor behind the campaign remains unidentified, though researchers observed consistent use of Spanish-language infrastructure and tooling throughout the operation.

Reference: https://www.dragos.com/blog/ai-assisted-ics-attack-water-utility

4.3 Hackers Use Fake Claude AI Installer Pages to Deliver Malware

Description –

Researchers have identified a large-scale malware campaign abusing fake Anthropic Claude AI installer pages to trick users into executing malicious commands on their systems.

The campaign, tracked as “InstallFix” or the Fake Claude Installer threat, leverages sponsored Google Ads to place malicious installer pages at the top of search engine results for terms such as “Claude Code” and “Claude Code install.”

According to researchers from Trend Micro, the attackers crafted highly convincing fake installation portals designed to closely resemble legitimate Claude AI setup documentation. Victims are instructed to execute operating system–specific commands for Windows or macOS, unknowingly triggering a multi-stage malware infection chain.

The malware campaign has reportedly targeted organizations and users across the United States, Malaysia, the Netherlands, and Thailand, impacting sectors including government, education, electronics, and food and beverage industries.

Researchers observed the malware using legitimate Windows tools such as mshta.exe and obfuscated PowerShell commands to evade detection and silently execute malicious payloads. The attack chain establishes persistence through scheduled tasks, performs system reconnaissance, steals browser and e-wallet data, and communicates with attacker-controlled infrastructure for additional payload delivery.

The attackers reportedly used victim-specific command-and-control URLs hosted on malicious infrastructure associated with prior RedLine Stealer campaigns, complicating network-level detection and blocking efforts.

Trend Micro noted that the campaign specifically exploits user trust in AI tools and developer installation workflows rather than targeting traditional software vulnerabilities. Researchers

warned that both technical and non-technical users are susceptible to these attacks due to the increasing popularity of AI development platforms and command-line installation methods.

Security experts recommend that organizations block known malicious domains and IP addresses, restrict legacy scripting tools such as mshta.exe, enforce DNS filtering, and educate users to avoid executing commands copied from sponsored search results or unofficial installation pages.

Reference:https://www.trendmicro.com/en_us/research/26/e/installfix-and-claude-code.html

Our Comprehensive Portfolio of Cyber Security Offerings

Service 1
SOC (Security Operation Center)

Deploying of SIEM, EDR, XDR, SOAR Technologies for Manage Detection and Response (MDR). 24x7 Incident Monitoring, Threat Intelligence & Threat Hunting, Incident Response

Service 7
Cloud Security Services

Cloud deployment, maturity assessments, migration, Securing Cloud by deploying the necessary controls

Service 6
Data Security

Data loss prevention, Data Discovery & Classification, Cyber Recovery Ransomware Strategy, Public Key Infrastructure, Data Encryption

Service 2
Enterprise Vulnerability Management

Vulnerability Management, Application Security, Penetration Testing, Red Teaming, DevSecOps

Service 5
Governance Risk and Compliance

Security Control effectiveness, identify solution to remediate risk through controls, frameworks, process and solutions, identify aplicable law and regulations and adopt industry framework & standards to meet compliance requirements

Service 3
IAM (Identity & Access Management)

Program setup & program governance, IAM strategy, architecture & roadmap, IAM maturity assessment, IAM product selection, consulting for role based access control/policy based access control strategy

Service 4
Network Security

Deploying perimeter devices like firewall, proxy, etc, implement zero trust strategy, Micro-Segmentation, Network security assessment

info.grc@crowe.ae
+971 52 373 4662
Level 21, The Prism, Business Bay, Dubai, UAE
Abu Dhabi | ADGM | DIFC | Sharjah
www.crowe.com/ae

Scan to Know more