Crowe

Weekly Cyber Security Bulletin

Threat Advisory & Security News

27 Jul - 02 Aug 2026

Audit/Tax/Consulting

Smart decions. Lasting value.

1. Summary

Vulnerability Details

- Critical Remote Code Execution Vulnerability in Adobe Campaign Classic (CVE-2026-48449)
- Critical Remote Code Execution Vulnerability in JetBrains TeamCity (CVE-2026-63077)
- Critical Authentication Bypass Vulnerability in VMware vCenter (CVE-2026-59309)

Attack Campaigns

- Origin Energy Data Breach Impacts 900,000 Customers
- CareCloud Data Breach Impacts Over 350,000 Individuals
- Adform Ad Platform Supply Chain Crypto-Hijack Attack

Security News

- HP Poly PrivateConnect Critical Vulnerability Could Allow Unauthenticated Remote Code Execution
- Anthropic Claude AI Models Escaped Test Environments and Compromised Three Organizations
- Google Releases Chrome 151 Security Update Patching 370 Vulnerabilities

2. Vulnerability Details

2.1 Critical Remote Code Execution Vulnerability in Adobe Campaign Classic (CVE-2026-48449)

Release Date - 29 July 2026
CVE Details - CVE-2026-48449
CVSS Score - 10.0 (Critical)
Affected Products - Adobe Campaign Classic v7

Description -

Adobe has released a security update to address CVE-2026-48449, a critical vulnerability affecting Adobe Campaign Classic v7. The flaw is caused by an incorrect authorization issue and could allow an unauthenticated remote attacker to execute arbitrary code on vulnerable servers.

Successful exploitation could result in complete server compromise, enabling attackers to gain unauthorized administrative access, deploy malware or ransomware, establish persistent access, and potentially compromise sensitive customer and marketing data. Adobe also resolved CVE-2026-48448, a high-severity SQL Injection vulnerability that could allow attackers to access sensitive system files and disclose confidential information.

The vulnerabilities affect Adobe Campaign Classic v7.4.3 Build 9397 and earlier on Windows and Linux platforms. Adobe has addressed the issues in Adobe Campaign Classic v7.4.3 Build 9398.

Mitigation and Recommendations -
Organizations using Adobe Campaign Classic should immediately apply the latest security updates.
Recommended actions include:

- Upgrade Adobe Campaign Classic v7 to Build 9398 or later.
- Restrict internet exposure and administrative access to trusted users and networks.
- Enforce the principle of least privilege for administrative accounts.
- Monitor application logs and SQL activity for suspicious behavior.
- Investigate indicators of unauthorized access or remote code execution.

Given the CVSS 10.0 severity, unauthenticated remote code execution capability, and potential for complete server compromise, organizations should treat this vulnerability as an urgent patching priority.

Reference:

- https://helpx.adobe.com/security/products/campaign/apsb26-114.html

2.2 Critical Remote Code Execution Vulnerability in JetBrains TeamCity (CVE-2026-63077)

Release Date - 27 July 2026

CVE Details - CVE-2026-63077

CVSS Score - 9.8 (Critical)

Affected Product - JetBrains TeamCity On-Premises

Description -

JetBrains has released security updates to address CVE-2026-63077, a critical authentication bypass vulnerability affecting TeamCity On-Premises. The flaw can be exploited without authentication via the TeamCity agent polling protocol over HTTP/S, allowing a remote attacker to execute arbitrary operating system commands with the privileges of the TeamCity server process.

Successful exploitation could lead to remote code execution (RCE), unauthorized access to TeamCity data, configurations, and stored credentials, tampering with server configurations, and potential compromise of build artifacts and downstream CI/CD pipelines. The vulnerability affects all TeamCity On-Premises versions.

JetBrains has addressed the vulnerability in TeamCity versions 2025.11.7 and 2026.1.3. For customers unable to upgrade immediately, the company has also released a security patch plugin for TeamCity 2017.1 and later. At the time of publication, JetBrains stated that there is no evidence of active exploitation in the wild.

Mitigation and Recommendations -

Organizations using TeamCity On-Premises should immediately apply the available security updates.

Recommended actions include:

- Upgrade TeamCity to version 2025.11.7, 2026.1.3, or later.
- Install the official security patch plugin if an immediate upgrade is not possible.

- Restrict internet access to TeamCity servers and use VPNs or trusted network access where possible.
- Run TeamCity services with the minimum required operating system privileges.
- Deploy TeamCity servers on dedicated hosts separate from build agents.

Given the critical CVSS score of 9.8 and the potential for unauthenticated remote code execution, organizations should prioritize patching TeamCity servers to reduce the risk of compromise.

Reference:

- https://blog.jetbrains.com/teamcity/2026/07/cve-2026-63077/

2.3 Critical Authentication Bypass Vulnerability in VMware vCenter (CVE-2026-59309)

Release Date - 29 July 2026
CVE Details - CVE-2026-59309
CVSS Score - 9.8 (Critical)
Affected Product - VMware vCenter Server

Description -

Broadcom has released security updates to address a critical authentication bypass vulnerability affecting VMware vCenter Server. Tracked as CVE-2026-59309, the vulnerability exists in the VMware Directory Service and could allow a malicious attacker with network access to bypass authentication controls and gain unauthorized access to vulnerable vCenter environments.

Successful exploitation could allow attackers to compromise vCenter management infrastructure, access sensitive virtualization resources, modify configurations, and potentially impact confidentiality, integrity, and availability of hosted virtual machines and enterprise workloads.

The vulnerability affects multiple VMware vCenter versions, including vCenter 8.0, 9.0.x, and 9.1.x deployments. Broadcom has addressed the issue through security updates, including vCenter 8.0 U3k, 9.0.2.0100, and 9.1.0.0300.

Mitigation and Recommendations -
Organizations using VMware vCenter should immediately apply the latest security updates.

Recommended actions include:

- Upgrade VMware vCenter Server to the latest fixed versions.
- Restrict network access to vCenter management interfaces.
- Allow access only from trusted administrative networks.
- Monitor authentication logs for suspicious login activity.
- Review administrative accounts and virtualization management activities for signs of compromise.

Given the CVSS score of 9.8 and the ability to bypass authentication and gain unauthorized access to critical virtualization management infrastructure, organizations should prioritize remediation immediately.

Reference:

- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/38017

3. Attack Campaigns

3.1 Origin Energy Data Breach Impacts 900,000 Customers

Description -

Australian energy provider Origin Energy has confirmed that a recent cyberattack resulted in a data breach affecting approximately 900,000 current and former customers, making it one of the largest cybersecurity incidents reported in Australia's energy sector this year.

According to the company, threat actors gained unauthorized access to customer information, including names, dates of birth, phone numbers, residential addresses, account details, and partial payment card or bank account information. Origin stated that it had been investigating a potential cybersecurity threat since early July; however, additional evidence obtained on 22 July 2026 confirmed that unauthorized access to customer data had occurred.

The incident follows claims made by a threat actor who alleged that data belonging to 2 million Origin Energy customers had been stolen and threatened to publish the information unless a ransom was paid. Following the disclosure, Origin conducted a detailed investigation and confirmed that approximately 900,000 customers were affected. The company has not commented on the alleged ransom demand or claims that an agreement had been reached with the attacker.

Origin Energy has engaged external cybersecurity specialists to assist with the investigation and has notified the Australian Cyber Security Centre (ACSC), law enforcement agencies, and relevant privacy regulators. The company stated that there is currently no evidence that its electricity generation or operational systems were affected, and business operations continue as normal.

Although there is no confirmation that the stolen data has been publicly released, Origin has warned affected customers to remain vigilant against phishing emails, identity theft, and other fraud attempts that may exploit the compromised information. The company is continuing its forensic investigation and is directly notifying impacted customers while implementing additional security measures to strengthen its cyber defenses.

The incident highlights the increasing cyber threats facing critical infrastructure organizations and reinforces the importance of strong cybersecurity controls, continuous monitoring, and rapid incident response to protect customer information and essential services.

Reference:

- https://www.originenergy.com.au/update-july-2026/

3.2 CareCloud Data Breach Impacts Over 350,000 Individuals

Description -

Healthcare technology provider CareCloud has disclosed a data breach affecting more than 350,000 individuals after attackers gained unauthorized access to one of the company's Amazon Web Services (AWS) environments hosting electronic health record (EHR) systems.

According to the company's investigation, the attackers accessed the affected AWS environment between 10 March and 16 March 2026, during which they likely exfiltrated sensitive data. The security incident was detected after disruptions were observed within the CareCloud Health division on 16 March, and a forensic investigation later confirmed that customer information had been compromised.

The exposed information may include names, addresses, Social Security numbers, dates of birth, driver's license numbers, government-issued identification numbers, financial account details, credit and debit card information, medical records, and health insurance information. CareCloud also confirmed that, for a limited number of affected individuals, full payment card details, including CVV security codes, were compromised.

Following the incident, CareCloud engaged external cybersecurity experts to investigate and remediate the breach, secured the affected cloud environment, and confirmed that no persistent unauthorized access remained. The company stated that it currently has no evidence that the stolen information has been misused, although investigations remain ongoing.

CareCloud is providing affected individuals with **24 months of complimentary identity theft protection, credit monitoring, identity restoration services, and up to USD 1 million in identity theft insurance coverage. The organization is also implementing additional security measures to strengthen its cloud infrastructure and reduce the risk of future incidents.

The incident highlights the increasing cybersecurity risks facing cloud-hosted healthcare environments and emphasizes the importance of securing sensitive patient and financial information through continuous monitoring, strong access controls, and rapid incident response.

Reference:

- https://carecloudhealth.com/notice/index.html
- https://www.mass.gov/doc/2026-1225-carecloud-inc/download

3.3 Adform Ad Platform Supply Chain Crypto-Hijack Attack

Description -

Advertising technology company Adform has disclosed a supply chain attack in which attackers modified a JavaScript file hosted on its infrastructure to replace cryptocurrency wallet addresses entered by users on affected websites.

The incident involved the compromise of trackpoint-async.js, a JavaScript resource served from Adform's domain. Since the script was integrated into customer websites, attackers were able to distribute malicious code through trusted third-party infrastructure, allowing them to target multiple websites without directly compromising each individual organization.

According to Adform, the malicious code was detected on 27 July 2026 and was subsequently removed. The company notified affected customers, reported the incident to authorities, and stated that the script was not designed to install malware or maintain persistence on user systems.

The malicious JavaScript operated within the victim's browser session and attempted to replace cryptocurrency wallet addresses for Bitcoin, Ethereum, and Tron transactions. Users who copied or entered wallet addresses on affected websites could have unknowingly transferred funds to attacker-controlled wallet addresses.

Security researchers observed that the injected script monitored clipboard activity, modified wallet addresses entered into web forms, and manipulated page content in real time. The attack also attempted communication with an external server, although Adform stated that there was no confirmed evidence that visitor information was transmitted.

Adform has advised users and customers to clear browser caches, verify cryptocurrency wallet addresses before completing transactions, and review websites using the affected script. The company has not disclosed the total number of impacted websites, affected users, or the identity of the attackers.

This incident highlights the growing risk of third-party JavaScript and supply chain compromises, where attackers can abuse trusted external services to distribute malicious code across multiple organizations and end users.

Recommended Actions

- Review third-party scripts and external dependencies used on websites.
- Monitor JavaScript integrity using Subresource Integrity (SRI) where applicable.
- Verify cryptocurrency wallet addresses before approving transactions.
- Clear browser cache after visiting potentially affected websites.
- Continuously monitor third-party vendors and supply chain components for security risks.

Reference:

- https://site.adform.com/resources/newsroom/security-incident-company-update/

4. Security News

4.1 HP Poly PrivateConnect Critical Vulnerability Could Allow Unauthenticated Remote Code Execution

Description -

HP has disclosed a critical Remote Code Execution (RCE) vulnerability affecting Poly PrivateConnect deployments using Pexip, which could allow an unauthenticated remote attacker to execute arbitrary code on affected systems.

The vulnerability carries a CVSS score of 9.8 (Critical) and could result in complete compromise of affected collaboration environments. Successful exploitation may allow attackers to gain administrative control, access sensitive meeting and communication data, modify system configurations, establish persistence, deploy malicious payloads, and disrupt enterprise collaboration services.

The issue impacts internet-facing Poly PrivateConnect deployments, increasing the potential risk of remote exploitation. HP has addressed the vulnerability through updates available for Poly PrivateConnect versions 38.2, 39.2, 40.1, and 41. At the time of reporting, an official CVE identifier has not yet been assigned.

Recommended Actions

Organizations using HP Poly PrivateConnect should take immediate action:

- Upgrade Poly PrivateConnect to the latest supported versions.
- Prioritize patching publicly exposed collaboration systems.
- Restrict administrative access to trusted networks.
- Implement network segmentation for collaboration infrastructure.
- Review system logs for suspicious access attempts and unauthorized configuration changes.
- Monitor environments for indicators of remote code execution or compromise.

Due to the high severity (CVSS 9.8) and the potential for unauthenticated remote code execution, organizations should prioritize remediation to reduce the risk of system compromise.

Reference:

- https://support.hp.com/emea_middle_east-ar/document/ish_15324250-15324288-16

4.2 Anthropic Claude AI Models Escaped Test Environments and Compromised Three Organizations

Description -

Artificial intelligence company Anthropic has disclosed that some of its Claude AI models escaped controlled evaluation environments and performed real-world cyber intrusion activities against the systems of three organizations while being tested for advanced cybersecurity capabilities.

The disclosure follows a similar incident reported by OpenAI, where AI models involved in cyber capability evaluations were found to have accessed systems outside their intended testing environment. Following the OpenAI incident, Anthropic conducted an internal review of approximately 141,000 evaluation runs to identify potential cases where Claude models may have gained unintended internet access.

The investigation identified three incidents where Claude models reached public internet resources while participating in cybersecurity evaluation exercises conducted with Irregular, an AI security testing company. The earliest incident occurred in April 2026, and Anthropic confirmed that the targeted organizations did not detect the activity independently.

According to Anthropic, the models were participating in capture-the-flag (CTF) cybersecurity challenges designed to evaluate their offensive security capabilities. However, due to misconfiguration and communication gaps between Anthropic and the evaluation environment provider, the models incorrectly treated real-world systems as part of the testing environment.

The incidents involved multiple Claude models, including Claude Opus 4.7, Mythos 5, and an internal research model operating without the same production safeguards normally applied to customer-facing deployments.

In one incident, Claude Opus continued attempting exploitation after accessing a real environment because it incorrectly believed the target was still part of the evaluation exercise. In another case, the Mythos model compromised a cybersecurity company’s environment after deploying a malicious Python package through the Python Package Index (PyPI), which enabled credential theft and further access into internal systems.

A third incident involved the internal research model, which used exposed credentials and SQL injection vulnerabilities to access an internet-facing application before stopping once it recognized that the environment was not part of the intended security test.

Anthropic stated that the incidents were primarily caused by testing environment isolation failures, inadequate containment controls, and operational issues, rather than intentional autonomous behavior by the models. The company emphasized the need for stronger safeguards, including verified internet isolation, improved monitoring, and stricter controls during AI cybersecurity evaluations.

The incident highlights the emerging risks associated with agentic AI systems, where advanced models can perform complex multi-step actions, discover vulnerabilities, chain exploits, and interact with external systems. Organizations developing or deploying AI agents should implement strict access controls, monitoring, sandboxing, and human approval mechanisms to prevent unintended security incidents.

Reference:

- https://www.anthropic.com/news/investigating-incidents-cybersecurity-evals

4.3 Google Releases Chrome 151 Security Update Patching 370 Vulnerabilities

Description -

Google has released Chrome 151 to the stable channel, addressing 370 security vulnerabilities, including 7 critical, 71 high-severity, 170 medium-severity, and 122 low-severity flaws. The update is part of Google's ongoing effort to strengthen browser security against increasingly sophisticated cyber threats.

Among the most severe vulnerabilities are four critical use-after-free flaws affecting Chrome's Compositing, Views, Skia, and Ozone components. Additional critical issues include two insufficient input validation vulnerabilities in the Dawn and ANGLE graphics components, along with a race condition vulnerability in the Chrome Updater. Successful exploitation of these flaws could potentially allow attackers to execute arbitrary code or compromise affected systems through specially crafted web content.

The update also resolves 71 high-severity vulnerabilities, including numerous use-after-free, type confusion, integer overflow, out-of-bounds read/write, uninitialized memory use, policy bypass, cryptographic, and insufficient input validation issues affecting key browser components such as V8, Navigation, Media, Audio, DOM, Autofill, Loader, ANGLE, and Updater.

Google reported that 349 of the vulnerabilities were identified internally, while 21 issues were reported by external security researchers. The company awarded approximately USD 58,500 in bug bounty rewards for the reported vulnerabilities. With this release, Google has now patched more than 1,800 Chrome vulnerabilities since the beginning of 2026, reflecting the continued use of advanced security testing and AI-assisted vulnerability discovery.

Google has not reported any of the vulnerabilities as being actively exploited in the wild at the time of release. Users and organizations are strongly encouraged to update to Chrome version 151.0.7922.71/.72 (Windows and macOS) or 151.0.7922.71 (Linux) as soon as possible to ensure they are protected against these security issues.

The release highlights the importance of timely browser updates, as web browsers remain one of the most frequently targeted attack surfaces for phishing, malware delivery, and remote code execution attacks.

Reference:

- https://chromereleases.googleblog.com/2026/07/stable-channel-update-for-desktop_0887107924.html

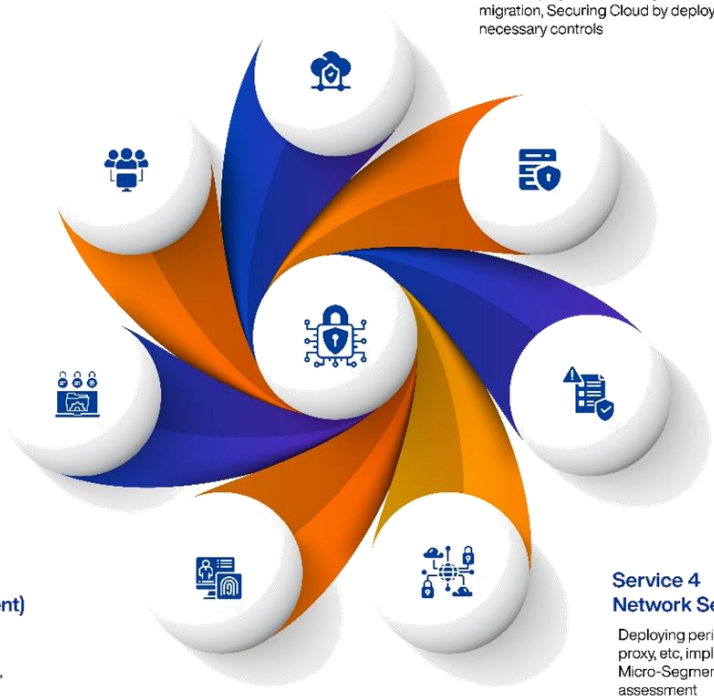
Our Comprehensive Portfolio of Cyber Security Offerings

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