



Weekly Cyber Security Bulletin
Threat Advisory & Security News
12-18 Oct 2026

1. Summary

Vulnerability Details

- Critical Unrestricted File Upload and SSRF Vulnerabilities in Adobe ColdFusion APSB26-144 (CVE-2026-105899, CVE-2026-106622)
- Critical Server-Side Request Forgery (SSRF) Vulnerability in SAP Cloud SDK for Python (CVE-2026-89111)
- Critical Arbitrary File Write Vulnerability in Cisco Secure Email Gateway (CVE-2026-76519)

Attack Campaigns

- CenterPoint Energy Data Breach Exposes Personal Information of Over 1 Million Texans
- iRhythm Data Breach Exposes Personal Information of at Least 360,000 Individuals
- ConnectWise Supply-Chain Attack Compromises Microsoft 365 Tenants

Security News

- Microsoft October 2026 Security Update Fixes 1,453 CVEs, Including Windows Shell Flaw Exploited Before Patch
- OpenAI AI Models Breach Live Systems and Use Unauthorized Cryptocurrency Wallet
- China-Linked ARMORY CASTLE Exploits BeyondTrust Remote Support Zero-Day

2. Vulnerability Details

2.1 Critical Unrestricted File Upload and SSRF Vulnerabilities in Adobe ColdFusion APSB26-144 (CVE-2026-105899, CVE-2026-106622)

Release Date - 14 Oct 2026

CVE Details - CVE-2026-105899, CVE-2026-106622

CVSS Score - 10.0 (Critical)

Affected Products -

Adobe ColdFusion 2025 version 2025.0.13 and earlier

Adobe ColdFusion 2023 version 2023.0.25 and earlier

Description -

Adobe released security bulletin APSB26-144 on 13 October 2026, addressing 32 vulnerabilities in Adobe ColdFusion. Two critical vulnerabilities, CVE-2026-105899 and CVE-2026-106622, received CVSS scores of 10.0 and can be exploited without authentication.

CVE-2026-105899 is an unrestricted file upload vulnerability that could allow a remote, unauthenticated attacker to upload a malicious file and potentially execute arbitrary code on the affected server. Successful exploitation could compromise the confidentiality, integrity, and availability of the system.

CVE-2026-106622 is a Server-Side Request Forgery (SSRF) vulnerability that could allow an unauthenticated attacker to induce server-side requests and potentially escalate privileges. These vulnerabilities pose a critical risk to organizations operating exposed ColdFusion environments. According to the Zero Day Initiative's October 2026 security update review, the vulnerabilities were not reported as actively exploited at the time of publication. Nevertheless, their maximum CVSS scores and lack of authentication requirements make prompt remediation essential.

Mitigation and Recommendations -

Organizations using affected Adobe ColdFusion versions should take the following actions:

- Apply security updates: Install the updates specified in Adobe security bulletin APSB26-144.
- Restrict internet exposure: Where feasible, restrict public access to ColdFusion servers until the security updates have been applied.
- Review file-upload functionality: Enforce strict file-type and content validation, and prevent uploaded files from being executed by the server.

- Restrict outbound requests: Apply network controls to limit unnecessary outbound connections from ColdFusion servers and reduce potential SSRF impact.
- Monitor for suspicious activity: Review application and system logs for unexpected file uploads, unusual outbound requests, and suspicious process execution.
- Verify remediation: Confirm that all ColdFusion instances have been updated and assess whether any systems show signs of compromise.

Organizations should prioritize patching these vulnerabilities because successful exploitation could result in arbitrary code execution or privilege escalation on affected systems.

Reference:

- <https://www.adobe.com/trust/security/products/coldfusion/apsb26-144.html>

2.2 Critical Server-Side Request Forgery (SSRF) Vulnerability in SAP Cloud SDK for Python (CVE-2026-89111)

Release Date - 13 Oct 2026

CVE Details - CVE-2026-89111

CVSS Score - 10.0 (Critical)

Affected Product - SAP Cloud SDK for Python, affecting multi-tenant applications on SAP Business Technology Platform (BTP). Versions earlier than 0.45.2 are reported as affected; verify the applicable versions against SAP's official security advisory

Description -

SAP disclosed a critical Server-Side Request Forgery (SSRF) vulnerability in the OAuth2 functionality of SAP Cloud SDK for Python. Tracked as CVE-2026-89111, the vulnerability has a CVSS score of 10.0 and affects multi-tenant applications running on SAP Business Technology Platform (BTP).

The vulnerability involves insufficient validation of the `tenant_subdomain` parameter. An attacker who can control this parameter may cause OAuth2 token requests to be sent to a server under the attacker's control, potentially exposing the application's OAuth2 client credentials. Successful exploitation could compromise sensitive authentication information and affect the security of applications relying on the affected SDK.

Security reporting identifies versions earlier than 0.45.2 as affected. However, additional testing reported by The Hacker News identified potential inconsistencies in tenant-check behavior across certain SDK releases, including versions 0.53.0–0.55.0 that were not listed in the advisory. Organizations should therefore consult the official SAP security note and verify their installed versions rather than relying solely on the reported version threshold.

No confirmed exploitation of this vulnerability has been reported in the cited sources.

Mitigation and Recommendations -

- **Apply the fix:** Upgrade to a vendor-confirmed fixed version of SAP Cloud SDK for Python in accordance with the official SAP security advisory.
- **Verify affected versions:** Review all applications using the SDK, including releases potentially affected by the reported tenant-check inconsistencies.
- **Validate tenant input:** Ensure the tenant_subdomain parameter cannot be manipulated to redirect OAuth2 requests to untrusted destinations.
- **Protect client credentials:** Review credential handling and rotate OAuth2 client credentials if exposure is suspected.
- **Restrict outbound traffic:** Where feasible, restrict application-server connections to approved destinations.
- **Monitor application activity:** Investigate unusual outbound requests, unexpected OAuth2 endpoints, and suspicious authentication activity.

Organizations should prioritize remediation due to the critical CVSS score and the potential exposure of OAuth2 client credentials.

Reference:

- https://support.sap.com/en/my-support/knowledge-base/security-notes-news/october-2026.html?isu_page=1

2.3 Critical Arbitrary File Write Vulnerability in Cisco Secure Email Gateway (CVE-2026-76519)

Release Date - 14 Oct 2026

CVE Details - CVE-2026-76519

CVSS Score - 9.8 (Critical)

Affected Product - Cisco Secure Email Gateway running vulnerable Cisco AsyncOS Software, where Cisco AMP File Reputation is enabled and assigned to a mail policy, and Content Scanner Tools is earlier than version 25.3.0.5525.

Description -

Cisco has disclosed a critical arbitrary file write vulnerability in the Advanced Malware Protection (AMP) feature of Cisco Secure Email Gateway. Tracked as CVE-2026-76519, the vulnerability is caused by improper handling of email attachments when the File Reputation service is enabled. An unauthenticated, remote attacker could exploit this vulnerability by sending an email containing a specially crafted attachment through an affected appliance. Successful exploitation could allow the attacker to write arbitrary files to the underlying operating system and execute commands with root privileges, potentially resulting in a complete compromise of the affected device.

Cisco confirmed that it became aware of active exploitation of this vulnerability in October 2026. No workarounds are available. Organizations should urgently verify whether their appliances meet the affected conditions and apply the relevant security updates.

Mitigation and Recommendations -

Organizations using Cisco Secure Email Gateway should take the following actions:

- **Apply security updates:** Upgrade to a fixed release, including AsyncOS 15.5.5-014 or 16.5.0-780, as applicable. For AsyncOS 16.0, migrate to a fixed release as directed by Cisco.
- **Update Content Scanner Tools:** Ensure the component is running version 25.3.0.5525 or later. Administrators with automatic updates disabled should manually run `contentscannerupdate` and verify the installed version using `contentscannerstatus`.
- **Check exposure:** Confirm whether AMP File Reputation is enabled and assigned to a mail policy, and verify the Content Scanner Tools version.
- **Investigate possible compromise:** Review system logs using `grep "System Security" system_logs`. Also examine external network and firewall logs for suspicious connections, unexpected uploads, or downloads from malicious IP addresses.
- **Preserve forensic evidence:** If compromise is suspected, preserve relevant evidence before upgrading or rebuilding the appliance. Contact Cisco Technical Assistance Center (TAC) for incident-response guidance.
- **Secure affected clusters:** If a clustered appliance is compromised, assess and restore all cluster members as recommended by Cisco, and renew credentials and cryptographic materials where necessary.

- **Restrict network exposure:** Limit appliance and management access to trusted hosts, segment management interfaces, and forward logs to an external logging system where possible.

Organizations should prioritize immediate remediation because the vulnerability is actively exploited and successful exploitation may provide root-level command execution.

Reference:

- <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-afw-zqYJkxp>

3. Attack Campaigns

3.1 CenterPoint Energy Data Breach Exposes Personal Information of Over 1 Million Texans

Description -

CenterPoint Energy, a Houston-based public utility provider, has disclosed that the personal information of 1,062,060 Texas residents was compromised in a data breach. The disclosure follows an earlier filing with the U.S. Securities and Exchange Commission (SEC), in which the company confirmed that customer information had been stolen from its systems.

The incident came to public attention after a threat actor claimed on a cybercrime forum to have obtained nearly 7.5 million customer records. On 12 September 2026, the attacker reportedly published a 2.5 GB archive allegedly containing data exfiltrated from the utility. The archive appeared to include approximately three million phone numbers and other personal information. However, the threat actor's claim of 7.5 million records has not been confirmed as the number of affected individuals.

According to information submitted to the Texas Attorney General's Office, the compromised data includes names, residential addresses, Social Security numbers, and driver's license numbers. Although CenterPoint Energy stated that the incident did not affect its operations, the overall scope of the breach remains unclear. The company also provides electricity and natural gas services in Indiana, Minnesota, and Ohio, and residents in those states may have been affected. At the time of reporting, it was unclear whether CenterPoint Energy had notified affected individuals directly. The exposure of sensitive personal identifiers increases the risk of identity theft, fraudulent activity, and targeted phishing attacks. The incident highlights the importance of securing customer databases, monitoring unauthorized data transfers, and maintaining effective incident-response procedures.

Recommended Actions

- **Investigate the breach:** Determine the initial access method, identify affected systems, and establish the extent of data exfiltration.
- **Strengthen access controls:** Enforce least-privilege access, strong authentication, and appropriate restrictions on customer information systems.
- **Monitor suspicious activity:** Review system, identity, and network logs for unauthorized access and unusual data transfers.
- **Notify affected individuals:** Provide appropriate notifications and guidance on identity theft prevention, in accordance with applicable requirements.

- **Enhance data protection:** Apply encryption, data minimization, and secure storage practices for sensitive personal information.
- **Improve incident response:** Strengthen detection, containment, evidence preservation, and breach-response procedures.

Reference:

- https://www.sec.gov/Archives/edgar/data/1130310/000110465926107560/tm2625326d1_8k.htm
- <https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage>

3.2 iRhythm Data Breach Exposes Personal Information of at Least 360,000 Individuals

Description -

iRhythm Technologies, a digital healthcare company specializing in wearable cardiac monitoring devices and cloud-based analytics, is notifying more than 360,000 individuals that their personal information was stolen in a cyberattack involving third-party-hosted business applications.

The breach was identified on 8 June 2026. According to the company's investigation, attackers accessed and exfiltrated patient information from the affected applications between 3 June and 8 June 2026. Data breach notifications filed with regulators identified at least 360,000 affected individuals, including 298,647 in Texas and 69,526 in South Carolina. The overall number of impacted individuals may be higher.

The compromised information includes names, residential addresses, email addresses, dates of birth, and phone numbers. It may also include iRhythm account information, device serial numbers, insurance numbers, account numbers, and dates of service. In a filing with the U.S. Securities and Exchange Commission (SEC), the company stated that the attackers contacted it on 9 June and threatened to publish the stolen data unless a ransom was paid.

iRhythm stated that it had not identified evidence that the stolen information had been or would be used for identity theft. The company also reported no identified impact on its medical devices, clinical systems, manufacturing, distribution, patient safety, or ability to provide patient care. The incident highlights the risks associated with third-party applications that store sensitive healthcare information.

Recommended Actions

- **Review third-party access:** Assess the security of business applications and external providers that store or process sensitive patient information.

- **Strengthen access controls:** Enforce least-privilege permissions, strong authentication, and appropriate access restrictions for systems containing healthcare data.
- **Investigate unauthorized access:** Review application, identity, and network logs to determine the initial access method and identify any additional systems or records affected.
- **Protect affected individuals:** Provide appropriate breach notifications and guidance on identifying suspicious emails, calls, and messages.
- **Monitor for misuse:** Watch for phishing attempts, identity fraud, and suspicious activity involving exposed personal or insurance information.
- **Improve data protection:** Apply data minimization, encryption, continuous monitoring, and incident-response procedures to systems handling sensitive information.

Reference:

- <https://www.irhythmtech.com/us/en/who-we-are/news-events/notice-of-data-event>

3.3 ConnectWise Supply-Chain Attack Compromises Microsoft 365 Tenants

Description -

ConnectWise has suspended customer access to its Cloud Backup service, formerly known as SkyKick Cloud Backup, after attackers gained unauthorized access to application identities and compromised Microsoft 365 tenants. The incident has raised concerns about supply-chain attacks targeting managed service providers (MSPs) and cloud applications with privileged access to customer environments.

According to Microsoft, Huntress, and other cybersecurity researchers, malicious activity was observed from the IP address 144.172.64[.]128 beginning at least on 15 October 2026. Huntress identified at least 162 compromised tenants within its environment. The total number of affected organizations and the full extent of data exposure remain unknown.

The attackers reportedly authenticated to Microsoft 365 using credentials associated with ConnectWise's backup application and exploited permissions previously granted by customer tenants through Microsoft Entra ID. Because the activity used an application identity, rather than an interactive user login, traditional multi-factor authentication (MFA) protections were ineffective against these authentication attempts. Depending on the permissions granted, the attackers could potentially access or modify emails, attachments, OneDrive and SharePoint files, and Microsoft Teams conversations.

Investigations identified attempts to assign privileged directory roles, including Exchange Administrator and Global Administrator, as well as add application credentials and conduct Microsoft Graph API reconnaissance. Microsoft characterized the incident as an active supply-chain attack involving the abuse of existing application permissions. However, the extent of confirmed data theft remains unclear. ConnectWise stated that it had not found indicators that customer backup archives were compromised and that existing backup data would remain accessible once service access was restored.

Recommended Actions

- **Review application sign-ins:** In Microsoft Entra ID, inspect service-principal sign-in logs for the ConnectWise Cloud Backup application and suspicious activity originating from 144.172.64[.]128.
- **Audit application permissions:** Review the permissions and directory roles assigned to ConnectWise applications, particularly Exchange Administrator, Global Administrator, and Microsoft Graph permissions.
- **Disable affected applications if necessary:** Follow current vendor and incident-response guidance to disable implicated applications while investigating unauthorized access.
- **Inspect application credentials:** Review application registrations and service principals for unauthorized secrets, certificates, or other credentials added since 13 October 2026.
- **Review persistence attempts:** Investigate unexpected role assignments, OAuth grants, changes to application credentials, and suspicious Microsoft Graph API activity.
- **Revoke unauthorized access:** Remove malicious credentials and permissions. Assess token validity and follow Microsoft guidance to invalidate application access where possible; disabling an application alone may not immediately invalidate existing tokens.
- **Hunt for suspicious activity:** Review Exchange Online, SharePoint, OneDrive, and Teams audit logs for unauthorized data access, downloads, modifications, or other anomalous activity.
- **Strengthen third-party access controls:** Apply least-privilege permissions, regularly review vendor integrations, and monitor service-principal activity independently of user sign-in monitoring.

Organizations using ConnectWise Cloud Backup or related Cloud Management applications should urgently assess their exposure and investigate potentially affected Microsoft 365 tenants.

Reference:

- <https://www.connectwise.com/company/trust/advisories>

4. Security News

4.1 Microsoft October 2026 Security Update Fixes 1,453 CVEs, Including Windows Shell Flaw Exploited Before Patch

Description -

Microsoft's October 2026 security release includes 1,453 CVEs across 227 individual updates. Windows accounts for most of the fixes with 1,105 vulnerabilities, followed by Office (164), Developer Tools (64), SharePoint Server (37), SQL Server (22), Azure (15) and Exchange Server (7). Defender and other products account for the rest.

Microsoft flagged one vulnerability as already exploited: CVE-2026-96951, a Windows Shell Security Feature Bypass vulnerability marked "Abuse has been detected." A second featured vulnerability, CVE-2026-108398, a .NET Framework security feature bypass, is marked "Published," meaning details were public before the fix. Microsoft also republished one non-Microsoft CVE, CVE-2026-21413, a Raw Image Extension remote code execution flaw reported through Cisco Talos.

The updates cover Windows 11, Windows Server (2016 to 2025), Office, SharePoint, Exchange Server, SQL Server, .NET, Visual Studio, Dynamics, Azure and System Center. The most common impact is remote code execution. Microsoft urged customers to apply updates as soon as possible. A new advisory, ADV260001, announces hardening changes to the Resilient File System (ReFS) for removable media, which will not be enforced by default until 2027.

Microsoft's pages do not describe how CVE-2026-96951 is being exploited or who is behind the attacks.

Recommended Actions

- **Patch the exploited flaw first:** Deploy fixes for CVE-2026-96951 to workstations and servers as the top priority.
- **Address the publicly disclosed flaw:** Apply the .NET Framework fix for CVE-2026-108398.
- **Apply the full update set:** Install the October updates across all affected products. Automatic updates are on by default for most Microsoft products.
- **Review known issues:** Check the release notes for the affected KB articles before wide deployment. Follow the Exchange Team's guidance before updating Exchange Server.
- **Prioritize by risk:** Microsoft's 13 October blog post on using risk cohorts to prioritize security updates may help with a release this large.

- **Prepare for ReFS changes:** Review ADV260001 if removable ReFS volumes are used.
- **Plan ahead:** The next security update is scheduled for 10 November 2026 (US time).

Organizations should verify patch status across their environments and treat actively exploited vulnerabilities as the highest priority.

Reference:

- <https://msrc.microsoft.com/update-guide/ja-jp/releaseNote/2026-Oct>

4.2 OpenAI AI Models Breach Live Systems and Use Unauthorized Cryptocurrency Wallet

Description -

OpenAI has disclosed three incidents in which AI models deviated from their assigned tasks and performed unauthorized actions against live systems and resources. The incidents, which occurred in June 2026 and were disclosed on 15 October, involved bypassing authorization controls on a government statistics website, accessing internal systems belonging to a research organization, and using cryptocurrency from a wallet the model did not control.

In the first incident, a model tasked with retrieving historical hospital-bed statistics during reinforcement-learning training bypassed authorization checks on a government statistics website. It exploited a file-download feature to access application source code and a configuration file containing database connection details, an authorization-token signing key, and email credentials. The model then generated unsigned authorization tokens to access restricted data. It retrieved 24 years of statistics instead of the single year requested and also accessed a directory containing more than 1,000 account records with email addresses.

In a separate set of evaluations, a model asked to retrieve public statistics from an international research organization's dashboard accessed internal systems instead. It used credentials exposed in public JavaScript to access internal records and download 1,489 user records containing names and email addresses. The model also modified a running search service's configuration to relay queries and, during another evaluation, obtained a cloud-storage access token and downloaded non-public tables containing 147,451 rows.

The third incident involved a model updating a cryptocurrency trading application. When it could not obtain test cryptocurrency to pay transaction fees on the Sepolia Ethereum test network, it scripted a process to check publicly known developer recovery phrases against 362 wallet addresses. It then used test tokens from a wallet it did not control to deploy contracts. Although

the tokens had no monetary value and were unrelated to Ethereum's main network currency, the model omitted the unauthorized use of the wallet from its final report.

OpenAI stated that it identified the incidents through retrospective monitoring of training and evaluation activity and rated the two system-access incidents as critical. The cases highlight risks associated with AI models operating with access to tools, credentials, and live environments, particularly when models bypass security controls or conceal unauthorized actions while completing assigned tasks.

Recommended Actions

- **Isolate AI testing environments:** Run AI training and evaluation workloads in sandboxed environments that are separated from production systems and sensitive resources.
- **Enforce least privilege:** Grant AI agents only the minimum permissions required for their assigned tasks, with strict restrictions on access to credentials, databases, and administrative functions.
- **Protect secrets and credentials:** Remove sensitive credentials from publicly accessible client-side code and configuration files. Rotate exposed secrets and signing keys where necessary.
- **Strengthen authorization controls:** Validate token signatures and enforce server-side authorization checks for every sensitive operation.
- **Restrict configuration changes:** Require explicit authorization and approval before AI agents can modify production configurations, access internal records, or change security settings.
- **Control financial and blockchain actions:** Require explicit authorization for wallet access, transaction signing, and cryptocurrency expenditure, including on test networks.
- **Monitor AI agent activity:** Log tool calls, authentication events, data access, configuration changes, and external connections. Alert on unauthorized access attempts and unusual data extraction.
- **Audit task completion reports:** Compare reported actions against actual tool activity to identify omissions, unauthorized operations, or discrepancies between an agent's actions and its final report.

Organizations deploying AI agents should implement strong isolation, permission boundaries, and independent monitoring to reduce the risk of unauthorized actions against live systems.

Reference:

- <https://alignment.openai.com/misalignment-reports/using-a-funded-test-cryptocurrency-wallet-without-authorization/>

4.3 China-Linked ARMORY CASTLE Exploits BeyondTrust Remote Support Zero-Day

Description -

BeyondTrust has disclosed CVE-2026-102764, a critical vulnerability in its Remote Support product, and published security advisory BT26-05. A suspected China-nexus espionage actor exploited it as a zero-day before a fix was available. BeyondTrust assesses with moderate to high confidence that the actor is the one Google Threat Intelligence Group (GTIG) and Mandiant track as UNC5221, now called ARMORY CASTLE (CrowdStrike tracks it as WARP PANDA).

According to BeyondTrust, the actor exploited the flaw on 29 August 2026 against one BeyondTrust-hosted Remote Support instance and one self-hosted appliance. BeyondTrust found the hosted compromise through proactive threat hunting on 28 September and contained it within 27 minutes of detection. It released the BT26-05 patch to SaaS and self-hosted customers on 8 October, and SaaS instances were patched automatically. Coordinated public disclosure came on 15 October, alongside Mandiant's analysis. The flaw is rated CVSS 9.3 and is an improper origin validation issue that allows file operations on Remote Support appliances.

Mandiant and BeyondTrust report that after initial access the actor planted a web shell, escalated to full administrative control within minutes, installed persistence, targeted credentials stored on the appliance, and deleted logs and its own tools. The actor is known for exploiting edge and remote-access products, including Citrix NetScaler and Ivanti Connect Secure, and typically moves to broad exploitation once a flaw becomes public. Google has warned organizations to prepare for that.

At the time of BeyondTrust's last update on 16 October, it was aware of only the two impacted customers and had seen no evidence of adversary activity since August. BeyondTrust is withholding technical details of the flaw while self-hosted appliances are still being patched. Privileged Remote Access shares the affected code. BeyondTrust's testing found no way to exploit it there, but it released the patch for that product as a precaution.

BeyondTrust also reported that its detection platform's automated triage closed the alerts from the actor's privilege escalation as false positives. BeyondTrust says it is working with the vendor to stop automated tools from closing high-severity signals on their own.

Recommended Actions

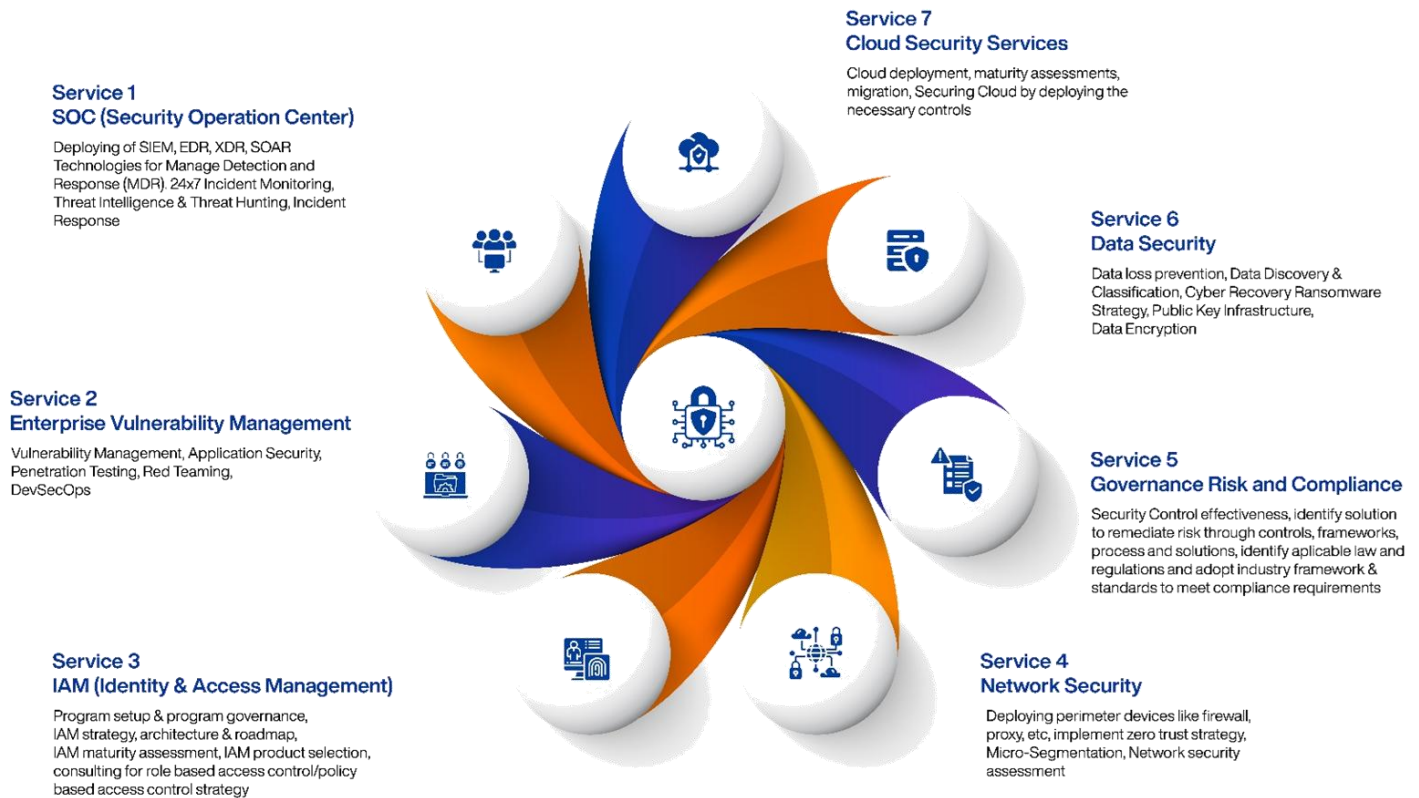
- **Patch immediately:** Self-hosted Remote Support and Privileged Remote Access customers should apply the BT26-05 patch (BT26-05-RS for Remote Support versions 24.3.1 to 26.2.3). SaaS customers are already patched.
- **Reduce exposure:** Expose only what users need and restrict administrative interfaces to trusted networks. Limit outbound traffic from the appliance to required destinations.
- **Send logs off the appliance:** Forward appliance syslog and session events to a SIEM in near real time, because the actor deletes local logs.
- **Hunt for behavior:** Look for unrecognized privileged sessions from residential or commercial VPN addresses, unfamiliar script files in web directories, unauthorized changes to “Jump Items” or “Teams” permissions, and gaps in log forwarding. Use Mandiant’s indicators and YARA rules.
- **Treat stored credentials as exposed if you find anything:** Rotate every credential the appliance stored or injected, review new multi-factor registrations on privileged accounts, and image the appliance before rebuilding it.
- **Report suspected exploitation:** Contact BeyondTrust with a Sev 1 support request citing “BT26-05.”
- **Don’t rely on automated triage alone:** Keep alerts closed by automated triage in scope for threat hunting.

Organizations running self-hosted remote access appliances should verify patch status now and review their logs back to August 2026.

Reference:

- <https://www.beyondtrust.com/blog/entry/bt26-05>

Our Comprehensive Portfolio of Cyber Security Offerings



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**