Crowe

Weekly Cyber Security Bulletin

Threat Advisory & Security News

09 Nov – 15 Nov 2026

Audit/Tax/Consulting

Smart decions. Lasting value.

1. Summary

Vulnerability Details

- CVE-2026-120868: Memory overflow in Packet Processing can lead to unpredictable or erroneous behavior or Denial of Service in NetScaler ADC and NetScaler Gateway.
- CVE-2026-119618: Apache HTTP Server: mod_http2 heap corruption and Remote Code Execution (RCE) in assign_headers()
- CVE-2026-89103: Broken Access Control in SAP Gateway
- CVE-2026-123710: Red Hat Quay: Unauthenticated Registry Signing-Key Takeover via Service Key Rotation

Attack Campaigns

- Dentsu Digital: TONARIWA platform compromised through leaked administrator credentials
- TSMC: Employee personal information exposed through a cloud service provider
- Gootloader: International law-enforcement operation disrupts malware infrastructure

Security News

All United Data Breach Exposes Personal Data of Dutch Sports Club Members

SEGA: Third Party marketing provider breach exposes 2.19 million email addresses

French National Blood Service: Cyberattack Targets Refrigeration Systems at Three Sites

Microsoft 365 Outage Demonstrates the Security Importance of Service Availability

2. Vulnerability Details

2.1 CVE-2026-120868: Memory overflow in Packet Processing can lead to unpredictable or erroneous behavior or Denial of Service in NetScaler ADC and NetScaler Gateway.

Release Date: 13 November 2026

CVSS Score: 9.3 (Critical)

Affected Products:

The vulnerability affects:

- Citrix NetScaler ADC
- Citrix NetScaler Gateway

Affected versions include:

Product	Affected Versions
NetScaler ADC	Earlier than 14.1-73.57
NetScaler ADC	Earlier than 13.1-64.39
NetScaler ADC FIPS	Earlier than 14.1-73.58 FIPS
NetScaler ADC FIPS / NDcPP	Earlier than 13.1-37.293
NetScaler Gateway	Earlier than 14.1-73.57
NetScaler Gateway	Earlier than 13.1-64.39

Summary

A memory overflow vulnerability exists in the packet-processing functionality of NetScaler products. Successful exploitation can cause the appliance to enter an unstable state, behave unexpectedly, or crash, resulting in denial-of-service conditions. The vulnerability is remotely exploitable over the network and does not require special privileges or user interaction.

Impact

- Denial of Service (DoS)
- Service interruption
- Application delivery disruption
- Unexpected or erroneous appliance behavior
- Potential crash of affected NetScaler instances

Fixed Releases

Product	Fixed Version
NetScaler ADC / Gateway	14.1-73.57 and later
NetScaler ADC / Gateway	13.1-64.39 and later
NetScaler ADC FIPS	14.1-73.58 FIPS and later
NetScaler ADC FIPS / NDcPP	13.1-37.293 and later

Vendor Recommendation

- Identify all vulnerable NetScaler ADC and Gateway deployments.
- Upgrade to the applicable fixed release.
- Prioritize internet-facing appliances due to network-based exploitation risk.
- Verify upgrade completion and monitor appliance stability after remediation.

Reference:

Citrix NetScaler ADC and Citrix NetScaler Gateway Security Bulletin

Identify and remediate vulnerabilities for CVE-2026-120868 | Security Advisory | NetScaler

2.2 CVE-2026-119618: Apache HTTP Server: mod_http2 heap corruption and Remote Code Execution (RCE) in assign_headers()

Release Date: 11 November 2026

CVSS Score: 9.8 (Critical)

Affected Product:

Apache Software Foundation Products

- Apache HTTP Server versions 2.4.55 through 2.4.70
- mod_http2 / mod_h2 versions 2.0.8 through 2.0.42

Affected Conditions

The vulnerability affects systems where:

- HTTP/2 (h2 or h2c) is enabled.
- The mod_http2 module is loaded.
- The server is reachable by remote clients.

Not Affected

- Servers configured only for HTTP/1.1.

Summary

A race-condition vulnerability exists in the assign_headers() function of the mod_http2 module in Apache HTTP Server. Due to improper synchronization between HTTP/2 worker threads, one thread can modify memory owned by another thread, resulting in heap corruption. An unauthenticated remote attacker can exploit this flaw through specially crafted HTTP/2 requests to achieve remote code execution.

Impact

- Execute arbitrary code remotely.
- Completely compromise the web server.
- Access, modify, or steal sensitive data.
- Disrupt services and applications.
- Gain control of the affected server process without authentication.

Fixed Releases

Product	Fixed Version
Apache HTTP Server	**2.4.71** and later
mod_h2	Version containing the fix shipped with Apache HTTP Server 2.4.71

Reference:

Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project

2.3 CVE-2026-89103: Broken Access Control in SAP Gateway

Release Date: 10 November 2026

CVSS Score: 10.0 (Critical)

Affected Product:

SAP Gateway versions affected include:

- KRNL64NUC 7.22
- KRNL64NUC 7.22EXT
- KRNL64UC 7.22
- KRNL64UC 7.53
- KRNL64UC 8.04
- KERNEL 7.22
- KERNEL 7.54
- KERNEL 7.77
- KERNEL 7.93
- KERNEL 9.16
- KERNEL 9.20
- KERNEL 9.21

Summary

SAP Gateway improperly activates a default Access Control List (ACL) with elevated privileges. This behavior can incorrectly classify an external attacker as a trusted internal application server. An unauthenticated attacker with network access to the SAP Gateway can exploit this flaw to perform unauthorized actions within the SAP environment.

Impact

- Unauthorized access to SAP application resources.
- Execution of unauthorized actions without authentication.
- Compromise of confidentiality, integrity, and availability of the SAP landscape.
- Privilege escalation by masquerading as an internal SAP application server.

- Potential full compromise of business-critical SAP systems.

Vendor Recommendation

- Apply SAP Security Note 3798345 without delay.
- Disable or reconfigure the default SAP Gateway ACL where applicable.
- Implement strict ACLs allowing only trusted SAP application servers.
- Restrict SAP Gateway network access using firewalls, segmentation, and VPN controls.
- Review SAP Gateway logs for suspicious requests appearing to originate from trusted internal systems.

Reference:

SAP Security Patch Day - November 2026

2.4 CVE-2026-123710: Red Hat Quay: Unauthenticated Registry Signing-Key Takeover via Service Key Rotation

Release Date: 11 November 2026

CVSS Score: 9.8 (Critical)

Affected Product:

Affected versions of Red Hat Quay include:

- Quay 3.9.x prior to 3.9.28
- Quay 3.10.x prior to 3.10.28
- Quay 3.12.x prior to 3.12.24
- Quay 3.14.x prior to 3.14.10
- Quay 3.15.x prior to 3.15.9
- Quay 3.16.x prior to 3.16.7
- Quay 3.17.x prior to 3.17.7
- Quay 3.18.x prior to 3.18.3
- Red Hat Quay 5 deployments

Summary

A critical vulnerability exists in **Red Hat Quay** where an unauthenticated attacker can obtain an anonymous registry token, abuse the service key rotation endpoint, and install a trusted signing key under their control. Tokens signed with the malicious key are then accepted by the registry, allowing unrestricted access to repositories.

The flaw stems from insufficient validation of credentials used during service key rotation, enabling an attacker to take control of registry token signing without authentication.

Impact

- Read private container images from any repository.
- Push malicious images into repositories.
- Replace or overwrite repository tags.
- Maintain persistent access by installing signing keys without expiration.

- Compromise software supply chains that depend on affected registries.
- Potentially disrupt registry operations and authentication workflows.

Fixed Releases

Product Version	Fixed Release
Quay 3.9	3.9.28
Quay 3.10	3.10.28
Quay 3.12	3.12.24
Quay 3.14	3.14.10
Quay 3.15	3.15.9
Quay 3.16	3.16.7
Quay 3.17	3.17.7
Quay 3.18	3.18.3

Vendor Recommendation

- **Upgrade to the appropriate fixed Quay version immediately.**
- **Restrict access to the /keys endpoint using a reverse proxy, firewall, or load balancer so only trusted internal services can reach it.**
- **Review audit logs for:**
  - **service_key_rotate**
  - **service_key_delete**

  especially events involving keys with no expiration date.
- **Remove any unauthorized signing keys and verify registry integrity.**
- **Assess all private repositories for unauthorized image modifications or tag replacements.**

Reference:

CVE-2026-123710 - Red Hat Customer Portal

3. Attack Campaigns

3.1 Dentsu Digital: TONARIWA platform compromised through leaked administrator credentials

Description

Dentsu Digital, a Japanese digital marketing company, disclosed that its marketing platform TONARIWA suffered a cyberattack after threat actors gained access using leaked administrator credentials. The attackers successfully accessed the platform, performed privilege escalation, and potentially exfiltrated sensitive data stored within the environment. The compromised information included customer personal data and LINE Official Account integration tokens used by client organizations. The company temporarily suspended the TONARIWA service, isolated affected systems, and launched a forensic investigation.

Attack Methodology

- Compromise of Administrative Credentials: Threat actors obtained valid administrator credentials used within the TONARIWA platform infrastructure. By using legitimate credentials, attackers were able to bypass traditional security controls and gain trusted access to the environment.
- Unauthorized Access Through Valid Authentication: Instead of exploiting a software vulnerability, the attackers logged in using compromised administrator credentials, making the activity appear legitimate and significantly reducing the likelihood of immediate detection.
- Privilege Escalation Activities: After gaining initial access, the threat actors expanded their permissions within the environment through privilege escalation, allowing them to access additional systems, administrative functions, and sensitive data repositories.
- Access to Sensitive Customer and Integration Data: The attackers accessed databases containing customer personally identifiable information (PII), including names, dates of birth, and contact information. They also obtained access to LINE

integration tokens used by client organizations for official account management and communications.

- Data Exfiltration and Information Leakage: During the investigation, logs revealed evidence of external data transfers, indicating that information was extracted from the platform. Subsequent analysis confirmed that personal information belonging to customers of at least two client organizations had been exposed.
- Potential Abuse of Trusted Communication Channels: Because official LINE integration tokens were potentially exposed, attackers could have leveraged trusted communication channels to distribute fraudulent messages, conduct phishing campaigns, or impersonate legitimate organizations.

Key Takeaways

- Stolen Credentials Remain One of the Most Effective Attack Vectors: Modern cyberattacks increasingly rely on compromised accounts rather than software vulnerabilities. A single privileged account can provide attackers with extensive access to critical systems and sensitive information.
- Privileged Accounts Require Enhanced Protection: Administrator accounts represent high-value targets because they can grant access to multiple systems, applications, and databases. Organizations should treat privileged identities as critical assets requiring additional security measures.
- API Tokens and Integration Credentials Are Sensitive Data: Security programs often focus heavily on passwords while overlooking access tokens. This incident demonstrates that stolen API keys and integration tokens can be just as dangerous as compromised user credentials.
- Valid Account Abuse Can Be Difficult to Detect: When attackers use legitimate credentials, malicious activity may blend into normal administrative operations. Organizations should supplement authentication monitoring with behavioral analytics and anomaly detection.
- Third-Party Platform Breaches Can Impact Multiple Organizations: A compromise affecting a shared marketing or communication platform can expose data belonging to numerous client organizations, creating wider supply-chain and business ecosystem risks.

- Rapid Containment Significantly Reduces Further Damage: Prompt actions such as credential revocation, service suspension, infrastructure isolation, and forensic investigations help limit attacker movement and reduce additional data exposure.

Mitigation Recommendations

- Enable Multi-Factor Authentication (MFA) for All Administrative Accounts: Implement phishing-resistant MFA methods such as security keys or authenticator apps to prevent unauthorized access even if passwords become compromised.
- Regularly Rotate Administrative Passwords and Access Tokens: Frequently update privileged credentials, API keys, service account passwords, and integration tokens to minimize exposure from leaked credentials.
- Adopt the Principle of Least Privilege: Grant users and service accounts only the permissions necessary to perform their tasks. Regularly review and remove unnecessary administrative privileges.
- Protect and Inventory Third-Party Integrations: Maintain visibility into all connected applications, API integrations, and access tokens. Disable unused integrations and review permissions periodically.
- Implement Strong Credential Management Practices: Store privileged credentials within secure vaults such as privileged access management (PAM) solutions and prohibit credential sharing among administrators.

Reference:

Apology and Report Regarding the Possibility of Personal Information Leakage Due to Unauthorized Access in Our Company's "TONARIWA" | Dentsu Digital

3.2 TSMC: Employee Personal Information Exposed Through a Cloud Service Provider

Description

Taiwan Semiconductor Manufacturing Company (TSMC), the world's largest contract semiconductor manufacturer, disclosed that personal information belonging to some current and former employees was exposed after data stored with an external cloud service provider appeared on an unauthorized website. The company stated that there was no evidence of compromise within TSMC's internal systems, manufacturing operations, or customer environments. The exposed data was verified to match records maintained by a third-party cloud provider used by the company.

Threat actors subsequently advertised an alleged dataset containing approximately 46,000 employee records (around 6.9 GB of data) on underground forums and demanded 3 Bitcoin in exchange for the data. Reportedly exposed information included employee names, national identification numbers, addresses, phone numbers, email addresses, banking information, job titles, and emergency contact details.

Attack Methodology

- Compromise of Third-Party Cloud Environment: Threat actors gained access to employee data stored within an external cloud service provider rather than directly breaching TSMC's internal infrastructure. The exact intrusion method has not been publicly disclosed.
- Unauthorized Access to Employee Data Repositories: Attackers obtained access to cloud-hosted records containing personal information of current and former employees. The exposed records matched information maintained within the cloud provider's environment.
- Extraction of Sensitive Personal Information: Following access to the cloud-hosted data, threat actors allegedly extracted large volumes of employee information, including identity, contact, and banking-related details. Reports indicate the dataset contained approximately 46,000 records.
- Publication of Sample Data as Proof of Possession: To demonstrate the authenticity of the stolen information, attackers reportedly released a sample dataset containing employee records and related personal information on cybercrime forums.

- Extortion Through Underground Forums: Threat actors advertised the dataset for sale on cybercriminal marketplaces and demanded cryptocurrency payments, threatening public release of the complete dataset if no buyer emerged within a specified period.
- Incident Investigation and Employee Notification: Following discovery of the exposure, TSMC initiated an investigation, engaged external cybersecurity specialists, coordinated with the cloud provider and relevant authorities, and began notifying affected personnel.

Key Takeaways

- Third-Party Providers Can Become a Security Weak Point: Even when an organization's internal systems remain secure, attackers may target cloud vendors and external service providers that store sensitive business or employee information.
- Employee Data Is a Valuable Target for Cybercriminals: Personal information such as identification numbers, addresses, email accounts, and banking details can be used for identity theft, financial fraud, phishing campaigns, and social engineering attacks.
- Cloud Data Requires the Same Protection as Internal Data: Organizations must recognize that outsourcing data storage does not transfer accountability for data protection. Sensitive information remains the organization's responsibility regardless of where it is stored.
- Supply Chain and Vendor Risks Continue to Increase: Modern enterprises often rely on numerous cloud providers, SaaS platforms, and third-party services. A security incident affecting one provider can expose thousands of records without any compromise of the organization's core environment.
- Public Data Exposure Can Lead to Long-Term Risk: Once personal information appears on underground forums or public websites, affected individuals may face years of elevated risk from targeted scams, credential theft attempts, and financial fraud.

Mitigation Recommendations

- Conduct Thorough Third-Party Security Assessments: Regularly evaluate cloud service providers for compliance with security standards such as ISO 27001, SOC 2 Type II, and NIST Cybersecurity Framework controls before entrusting them with sensitive information.
- Implement Strong Cloud Access Controls: Enforce Multi-Factor Authentication (MFA), role-based access control (RBAC), and least-privilege principles across all cloud-hosted systems and third-party platforms.
- Encrypt Sensitive Employee Information: Ensure personal and financial information is encrypted both at rest and in transit using strong encryption standards such as AES-256 and TLS 1.2/1.3.
- Regularly Review Vendor Data Retention Practices: Limit the amount of employee data stored by external providers and ensure outdated records are securely deleted according to business and regulatory requirements.
- Strengthen Incident Response Coordination with Vendors: Establish contractual obligations requiring third-party providers to rapidly notify customers of suspected breaches, support forensic investigations, and cooperate during incident response activities.
- Educate Employees About Post-Breach Risks: Inform affected personnel about phishing attempts, identity theft schemes, fraudulent communications, and other threats that frequently follow personal data exposures.
- Monitor Financial and Personal Accounts for Suspicious Activity: Employees whose information may have been exposed should review banking activity, credit reports, government identity accounts, and online services for signs of unauthorized use.
- Review Cloud Security Configurations Regularly: Perform periodic cloud security audits, access reviews, and misconfiguration assessments to identify exposed storage, excessive permissions, or insecure integrations before attackers can exploit them.

Reference: Document

3.3 Gootloader: International Law-Enforcement Operation Disrupts Malware Infrastructure

Description

An international law-enforcement operation led by the U.S. Department of Justice (DOJ), Federal Bureau of Investigation (FBI), Europol, and multiple global partners successfully disrupted the infrastructure behind the Gootloader malware operation. Authorities removed malware from more than 100 compromised servers, seized domains used to distribute and control the malware, and dismantled key components of the criminal ecosystem that enabled ransomware attacks and cybercrime activities. Since 2018, Gootloader has infected at least 25,000 computers worldwide and has been linked to ransomware attacks causing approximately $28.8 million in losses across at least 44 U.S.-based victims.

The operation was conducted as part of Operation Endgame, a multinational initiative targeting malware-as-a-service and cybercrime infrastructure. Authorities also seized hundreds of servers and domains associated with related malware operations and identified more than 6.4 million stolen credentials stored within criminal infrastructure.

Attack Methodology

- Compromised Website Distribution Campaigns: Operators behind Gootloader compromised legitimate websites, particularly vulnerable WordPress sites, and used them to host malicious content designed to infect visitors.
- Search Engine Optimization (SEO) Poisoning: Threat actors manipulated search engine rankings so malicious websites appeared prominently in search results. Victims searching for legal agreements, contracts, or business documents were redirected to attacker-controlled content.
- Malicious File Download and Execution: Users were tricked into downloading what appeared to be legitimate legal or business documents. These files contained malicious code that executed on the victim's device and initiated the infection process.
- Deployment of Malware Loader Functionality: Once executed, Gootloader acted as a malware loader, providing attackers with an initial foothold and enabling the delivery of additional malicious payloads onto infected devices.

- Establishment of Persistent Access: Infected systems became part of a broader criminal infrastructure, allowing threat actors to maintain access and potentially deploy further tools, including ransomware, remote-access malware, and credential-stealing malware.
- Sale of Access to Other Cybercriminals: Gootloader operators reportedly sold access to compromised systems to ransomware groups and other threat actors, enabling follow-on attacks such as data theft, extortion, and ransomware deployment.
- Law-Enforcement Infrastructure Takedown: Through court-authorized actions, law-enforcement agencies seized domains, removed malware from servers, disrupted command-and-control infrastructure, and notified victims to prevent further abuse.

Key Takeaways

- Compromised Legitimate Websites Can Become Malware Distribution Platforms: Trusted websites, especially outdated or poorly secured WordPress installations, can be weaponized by attackers to distribute malware to unsuspecting users.
- Search Engine Results Cannot Always Be Trusted: Cybercriminals increasingly use SEO manipulation techniques to place malicious content in front of users searching for business documents, contracts, and common workplace resources.
- Malware Loaders Enable Larger Cybercrime Ecosystems: Gootloader itself may not perform ransomware attacks directly, but it provides access that enables ransomware operators, credential thieves, and other cybercriminal groups to launch subsequent attacks.
- Initial Access Brokers Continue to Drive Ransomware Threats: Cybercriminal groups increasingly specialize in gaining access to organizations and selling that access to other threat actors, making malware loaders highly valuable within the cybercrime economy.
- International Collaboration Is Essential for Combating Cybercrime: The successful disruption demonstrates how coordinated efforts between law enforcement, private-sector security companies, CERTs, and international partners can significantly impact global cybercriminal operations.
- Credential Theft Creates Long-Term Risks: Investigators identified more than 6.4 million stolen credentials within criminal infrastructure, highlighting how a single

malware infection can lead to account compromise, fraud, and future ransomware attacks.

Mitigation Recommendations

- Keep Websites and Content Management Systems Updated: Organizations using WordPress should promptly apply security patches, update plugins and themes, and remove unsupported components to reduce the risk of website compromise.
- Implement Multi-Factor Authentication (MFA): Enable MFA for administrative accounts, website management portals, remote-access services, and cloud platforms to reduce the impact of stolen credentials.
- Train Users to Verify Download Sources: Employees should download documents, software, and templates only from trusted and verified sources. Suspicious legal forms or business documents found through search engines should be carefully validated before opening.
- Regularly Scan Websites for Compromise: Organizations hosting public-facing websites should conduct routine vulnerability assessments, malware scans, and file integrity monitoring to identify unauthorized changes quickly.
- Change Passwords Following Suspected Infection: If a device is believed to have been infected, immediately reset credentials used on that system and review accounts for signs of unauthorized access.

Reference:

Office of Public Affairs | Gootloader Malware Disrupted in International Cyber Operation | United States Department of Justice

6.4 million victim datasets secured in international operation against malware networks - Gootloader, CastleRAT, and StealC malware targeted in latest Operation ENDGAME cyber strike | Europol

4. Security News

4.1 AllUnited Data Breach Exposes Personal Data of Dutch Sports Club Members

Executive Summary

Dutch sports management platform AllUnited, a widely used membership administration system for sports clubs and federations in the Netherlands, suffered a significant cyberattack that resulted in unauthorized access to membership databases. The breach reportedly affected data belonging to sports clubs and federations that use the platform for member administration, payments, registrations, and communications.

According to public reports, the attacker exploited a vulnerability in a registration frm connected to an AllUnited-managed environment and successfully copied data from the database. Exposed information may include names, addresses, email addresses, phone numbers, dates of birth, bank account details (IBANs), and potentially account credentials. More than 350 Dutch sports clubs reportedly filed breach notifications with the Dutch Data Protection Authority following the incident.

Incident Summary

AllUnited, a leading Duth sports administration platform used by hundreds of clubs and federations, suffered a cyberattack that resulted in unauthorized access to its membership database. The attacker exploited a vulnerability in a registration form, enabling the theft of personal information that may include names, addresses, email addresses, phone numbers, dates of birth, bank account details, and account credentials. The incident has reportedly impacted a large number of sports organizations across the Netherlands, with more than 350 clubs notifying the Dutch Data Protection Authority (AP). The breach highlights the growing cybersecurity risks associated with third-party service providers and the importance of securing public-facing applications that store sensitive member data.

Key Takeaways

1. Third-Party Platforms Are High-Value Targets

Organizations often entrust member, customer, or employee data to third-party service providers. A compromise of one vendor can affect hundreds or thousands of organizations

simultaneously. The AllUnited incident demonstrates the concentration risk associated with centralized membership management systems.

2. Personal Data Is Valuable to Cybercriminals

Even when financial information is not directly monetized, stolen personal data can be used for:

- Phishing attacks
- Identity theft
- Social engineering campaigns
- Account takeover attempts
- Financial fraud using trusted organizational branding

The exposure of contact information combined with membership details increases the likelihood of highly convincing scams.

3. Vulnerabilities in Public-Facing Applications Remain a Major Risk

The reported intrusion began through a vulnerability in a registration form, underscoring the importance of:

- Secure coding practices
- Regular vulnerability assessments
- Web application security testing
- Continuous monitoring of internet-facing systems

Organizations should treat public forms and portals as critical attack surfaces.

4. Rapid Detection and Response Matter

Reports indicate the vulnerability was identfied and addressed quickly after discovery. While remediation cannot undo data exposure, timely response helps prevent further compromise and limits organizational impact.

5. Users Should Remain Vigilant After a Breach

Affected individuals should:

- Chang passwords, especially if reused elsewhere
- Enable Multi-Factor Authentication (MFA)
- Monitor bank accounts and financial activity
- Be cautious of emails, calls, or SMS messages claiming to be from sports clubs or financial institutions
- Verify payment requests through official channels

Reference: Security incident at AllUnited

4.2 SEGA: Third Party marketing provider breach exposes 2.19 million email addresses

Executive Summary

SEGA Corporation has confirmed a large-scale data breach stemming from the compromise of Arara Message, a third-party email marketing and newsletter distribution provider used by SEGA and SEGA Fave. The incident resulted in the exposure of 2,196,044 email addresses associated with marketing and promotional newsletter subscriptions. Additionally, newsletter delivery-related information linked to approximately 92,273 email addresses may have been exposed and remains under investigation.

According to SEGA, the breach was limited to data stored within the third-party provider's environment and did not affect customer accounts, passwords, payment information, or other sensitive personal information. While no evidence of data misuse has been reported, the exposed email addresses could be leveraged for phishing, impersonation, and social engineering attacks targeting affected individuals. The incident highlights the growing cybersecurity risks associated with third-party vendors and supply chain dependencies

Incident Summary

SEGA Corporation disclosed that unauthorized actors gained access to systems operated by its third-party newsletter provider, Arara Message, after exploiting a web server vulnerability within the provider's infrastructure. As a result, attackers obtained **2.19 million email addresses** used for distributing newsletters and promotional content related to various SEGA products and events. Investigation findings also revealed that delivery-related information associated with approximately **92,273 email addresses** may have been compromised.

The affected newsletters were distributed between July and October 2026 and included communications related to titles such as CHUNITHM Mate, ONGEKI Re:Fresh Act.2, maimai Deluxe MAGiCAL, SEGA Lucky Draw promotions, and Tokyo Game Show announcements. SEGA emphasized that no customer names, residential addresses, birth dates, phone numbers, credit card information, or login passwords were exposed during the incident. Furthermore, email addresses associated with SEGA Account services were not impacted because they are managed through a separate system.

Although no malicious use of the exposed data has been identified, SEGA warned that threat actors could exploit the leaked email addresses to launch phishing campaigns

impersonating SEGA, SEGA Fave, or Arara. The company has suspended the use of the affected email distribution service and is continuing its investigation alongside the provider.

Key Takeaways

1. Third-Party Risk Remains a Major Cybersecurity Challenge: Organizations can suffer significant data exposure even when their own internal systems remain uncompromised. This incident underscores the importance of conducting rigorous vendor security assessments and continuous third-party risk monitoring.
2. Email Addresses Alone Can Be Valuable to Attackers: While no passwords or financial information were exposed, a database containing millions of verified email addresses can be used to conduct highly targeted phishing, spam, credential harvesting, and brand impersonation campaigns.
3. Supply Chain Attacks Continue to Expand: Cybercriminals increasingly target service providers because compromising a single vendor can provide access to data from multiple organizations and millions of users simultaneously.
4. Segmentation Helped Limit the Impact: SEGA's separation of its core account infrastructure from its marketing systems prevented exposure of account credentials and sensitive customer information, demonstrating the value of data segregation and security-by-design principles.
5. Users Should Remain Alert for Phishing Attempts: Affected individuals should treat unexpected emails, links, attachments, promotional offers, and password reset requests with caution, particularly those claiming to originate from SEGA, SEGA Fave, or Arara.

Reference:

Apology and Notice Regarding Personal Information Leakage Due to Unauthorized Access to Subcontracted Companies | Sega Corporation

4.3 French National Blood Service: Cyberattack Targets Refrigeration Systems at Three Sites

Executive Summary

The French Blood Establishment (EFS), France's national blood service, disclosed a cyberattack that impacted refrigeration monitoring and control systems at three of its facilities. The attack targeted a third-party refrigeration service provider rather than the blood service directly, enabling threat actors to manipulate temperature and defrost settings within cold-storage environments used to preserve plasma and blood-related products. Despite the potentially severe implications for public health, monitoring systems detected the anomalies in time, allowing personnel to intervene before any blood products or samples were damaged. Blood collection, processing, and distribution operations continued without interruption.

The incident highlights the growing cybersecurity risks associated with Operational Technology (OT), Industrial Control Systems (ICS), and internet-connected refrigeration infrastructure. It also demonstrates how attacks on third-party suppliers can create potentially critical disruptions to healthcare services and supply chains.

Incident Summary

On November 2, 2026, a cyberattack affected refrigeration monitoring and control systems deployed at three facilities operated by the French Blood Establishment (EFS). According to official statements, attackers gained access through a compromised refrigeration equipment supplier, widely reported to be Coolworld Rentals, rather than directly breaching EFS systems. The attack altered temperature and defrost thresholds in cold-storage rooms used to store plasma for transfusions, plasma used in medicine manufacturing, and biological samples. Some reports indicated that refrigeration systems were reprogrammed to extremely high temperature settings, potentially placing critical medical supplies at risk.

Fortunately, EFS's monitoring and alarm systems rapidly detected the abnormal activity, prompting staff to secure the stored materials and transfer products to alternative refrigeration units where necessary. As a result, no blood products were lost, no health impacts were reported, and healthcare services continued without disruption. Following the incident, EFS collaborated with ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) and the French Ministry of Health to investigate the attack,

strengthen monitoring measures, and disable remote access to affected refrigeration systems while forensic investigations continue.

Key Takeaways

1. Cyberattacks Can Have Direct Physical Consequences: Unlike traditional data breaches, this incident targeted operational technology controlling refrigeration systems. Such attacks can disrupt critical services and potentially endanger public safety if not detected quickly.
2. Third-Party Vendors Remain a Significant Risk: The compromise reportedly originated through a refrigeration equipment provider, demonstrating how supplier vulnerabilities can impact critical infrastructure and healthcare organizations.
3. Monitoring and Alerting Systems Prevented Operational Impact: Real-time alarms and environmental monitoring enabled EFS personnel to identify unauthorized changes rapidly and take corrective action before any products were damaged.
4. Healthcare OT and IoT Systems Require Stronger Protection: Hospitals, laboratories, blood banks, and pharmaceutical facilities increasingly depend on connected systems. Securing refrigeration controllers, remote monitoring platforms, and industrial devices is essential to maintaining operational resilience.
5. Segmentation and Incident Response Reduce Risk: The incident demonstrates the value of contingency planning, backup storage capabilities, network segmentation, and rapid incident response procedures for critical healthcare infrastructure.

Reference:

US Government Partners Urge Hardening Industrial Refrigeration and Cold Chain Monitoring Systems

4.4 Microsoft 365 Outage Demonstrates the Security Importance of Service Availability

Executive Summary

Microsoft experienced a major global outage affecting multiple Microsoft 365 services, including Outlook, Exchange Online, Microsoft Teams, SharePoint Online, Microsoft 365 Copilot, and Defender XDR. The disruption began on November 12, 2026, and impacted users across more than 70 countries, causing widespread service interruptions for businesses, government agencies, educational institutions, and other organizations worldwide.

Following an investigation, Microsoft confirmed that the outage was not caused by a cyberattack, ransomware incident, or AI-related malfunction. Instead, the disruption stemmed from a combination of a latent software defect, increased traffic load on networking gateways, and reduced server availability, which resulted in critical Microsoft 365 infrastructure becoming unresponsive.

Incident Summary

On November 12, 2026, Microsoft reported connectivity and availability issues impacting several core Microsoft 365 services worldwide. Initial reports centered on Exchange Online mailbox access failures, but the scope quickly expanded to include Outlook, Teams, SharePoint, Copilot, Intune, and security platforms such as Defender for Office 365 and Defender XDR. Organizations reported difficulties accessing email, collaboration tools, file-sharing services, and cloud productivity applications.

According to Microsoft's preliminary findings, the outage was triggered by a previously undetected software defect within Microsoft 365 networking gateway servers. The issue remained dormant for months before a combination of increased gateway load and reduced server capacity caused servers to become overwhelmed and fail. Automated recovery mechanisms subsequently propagated the issue across additional infrastructure, resulting in widespread service degradation. At the peak of the incident, a significant portion of gateway servers became unresponsive, disrupting services globally. Microsoft engineers implemented traffic redistribution, server recovery processes, health-check modifications, and infrastructure remediation measures before restoring services.

Key Takeaways

1. Not Every Major Outage Is a Cyberattack: Although outages of this scale often raise concerns about ransomware or nation-state activity, Microsoft confirmed that this incident resulted from internal technical failures rather than external malicious activity.
2. Single Points of Failure Can Have Global Impact: The incident demonstrates how failures within critical cloud infrastructure components can cascade across multiple services used by millions of organizations worldwide.
3. Cloud Dependency Increases Operational Risk: Organizations that rely heavily on cloud-based email, collaboration, identity, and productivity services can experience significant business disruption when providers encounter service failures.
4. Resilience and Business Continuity Planning Remain Critical: The outage highlights the importance of backup communication channels, continuity planning, alternate collaboration platforms, and incident response procedures for cloud service disruptions.
5. Cybercriminals Quickly Exploit Major Public Incidents: Following the outage, threat actors reportedly launched phishing campaigns impersonating Microsoft service notifications and outage recovery alerts in an attempt to steal user credentials. Organizations should remain vigilant against opportunistic cyber threats following high-profile incidents.

Reference:

PostIncidentReport.pdf

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