Crowe

Weekly Cyber Security Bulletin

Threat Advisory & Security News

02-08 Nov 2026

Audit/Tax/Consulting

Smart decions. Lasting value.

1. Summary

Vulnerability Details

- Eight Critical CVSS 10.0 Vulnerabilities Fixed in Apache Juneau 9.2.1
- Critical Remote Code Execution Vulnerability in Android (CVE-2026-58868)
- Critical Improper Authentication Vulnerability in WatchGuard AuthPoint Gateway (CVE-2026-121639)

Attack Campaigns

- Florida Department of Education Data Breach Exposes Personal Information of 4.9 Million People
- Frontline Education Data Breach Exposes Personal Information of Over 1.3 Million Individuals
- OpsShield Supply Chain Attack Distributes Malicious cPGuard Updates to Linux Servers

Security News

- OpenAI Says New GPT-6 Cyber Model Hunts Flaws Without Crossing the Line
- Google Releases Chrome 157 with 213 Security Fixes, Including Seven Critical Vulnerabilities
- DigiCert Reports Data Breach Exposing Business Customer Information Through Misconfigured Internal System

2. Vulnerability Details

2.1 Eight Critical CVSS 10.0 Vulnerabilities Fixed in Apache Juneau 9.2.1

Release Date - 03 Nov 2026

CVE Details - Eight CVEs rated CVSS 10.0 (Critical); an additional vulnerability, CVE-2026-73095, is rated CVSS 8.7 (High).

CVSS Score - 10.0 (Critical) - CVSS 4.0

Affected Products - Apache Juneau versions 9.2.0 and earlier, including affected modules embedded in shaded and aggregate artifacts.

Description -

The Apache Juneau Project has released version 9.2.1 to address nine security vulnerabilities affecting Apache Juneau versions up to and including 9.2.0. Eight of these vulnerabilities received CVSS 4.0 scores of 10.0 from the Apache CNA, while the remaining vulnerability, CVE-2026-73095, received a score of 8.7.

The vulnerabilities affect different components and functionalities of Apache Juneau, with potential security impacts including unauthorized information disclosure, authentication and authorization bypass, cross-site scripting (XSS), request header injection, and path traversal. Depending on the affected functionality and deployment configuration, successful exploitation could expose sensitive information or compromise application security.

Although the eight vulnerabilities received the maximum CVSS 4.0 score, Apache's own severity assessments range from Low to Important. Some vulnerabilities also require specific deployment conditions or configurations to be exploitable. For example, certain issues depend on access to application logs, request variables being included in page chrome, application code constructing HTTP headers or redirects from request data, or specific DirectoryResource settings being enabled.

The Apache project also identified changes introduced in version 9.2.1 that may affect existing applications. These include changes to request-body size handling, error-response details, and the handling of the content query parameter. The upgrade additionally requires application developers to review redirect-handling implementations and custom HTTP client configurations.

According to the available reporting dated 6 November 2026, none of the nine vulnerabilities were listed in the CISA Known Exploited Vulnerabilities (KEV) catalogue. NVD records were marked as Deferred, with the Apache CNA's CVSS 4.0 scores available but no CVSS 3.1 scores published.

Mitigation and Recommendations

Organizations using Apache Juneau should take the following actions:

- **Apply security updates:** Upgrade all affected Apache Juneau components to version **9.2.1** or later.

- **Identify embedded components:** Review Maven dependencies, including juneau-shaded and other aggregate artifacts that may contain vulnerable modules.
- **Review application configurations:** Check DirectoryResource settings, particularly allowViews, allowUploads, and allowDeletes, and disable unnecessary functionality.
- **Restrict sensitive information exposure:** Review application logs and remove sensitive credentials or secrets that may have been exposed. Rotate affected credentials where necessary.
- **Review redirect handling:** Replace unsafe sendRedirect() implementations with sendSafeRedirect() where redirect targets are derived from request data.
- **Validate custom HTTP clients:** Review applications using custom HTTP clients and implement appropriate redirect-handling protections.
- **Test application compatibility:** Validate the updated request-size limits, error-response behavior, and content query parameter handling before production deployment.
- **Monitor suspicious activity:** Review application logs and access records for unauthorized requests, unusual file access, and potential information disclosure.

Organizations should prioritize upgrading to Apache Juneau 9.2.1, particularly where affected modules are exposed through internet-facing applications. The update addresses multiple security weaknesses, and the differing exploitability conditions should be assessed against each organization's deployment.

Reference:

- https://lists.apache.org/thread/j05q7vw08j48o96tdlzcsd4sozx1lyl6

2.2 Critical Remote Code Execution Vulnerability in Android (CVE-2026-58868)

Release Date - 03 Nov 2026

CVE Details - CVE-2026-58868

CVSS Score - 9.8 (Critical)

Affected Product -

- Android 14, Android 15, Android 16, and Android 17

Description -

Google has released its November 2026 Android security updates to address a critical vulnerability that could allow remote code execution (RCE) without requiring any user interaction. Tracked as CVE-2026-58868, the vulnerability affects Android versions 14 through 17 and is

associated with a heap-based buffer overflow in the FrameDecoder.cpp file, specifically within the onOutputReceived function.

The vulnerability could result in an out-of-bounds write, potentially allowing a remote attacker to execute arbitrary code on an affected device without requiring user interaction. Google has classified the issue as Critical, with its severity assessment assuming that Android's built-in security protections and Google services are disabled or bypassed.

Google addressed the vulnerability through its November 2026 Android security bulletin. Devices receiving the security patch level 2026-11-01 or later include the fix for CVE-2026-58868. However, the availability of updates depends on individual device manufacturers and mobile carriers.

As of 4 November 2026, Google had not reported any active exploitation of the vulnerability. The flaw was also not listed in the CISA Known Exploited Vulnerabilities (KEV) catalogue as of its 3 November update. Google has not published details explaining how an attacker could reach the vulnerable code.

Mitigation and Recommendations

Android users and organizations managing Android devices should take the following actions:

- **Apply security updates:** Install the latest Android security update provided by the device manufacturer or mobile carrier.
- **Verify patch levels:** Check the Android security update date under Settings → About phone → Android version. Ensure the security patch level is 2026-11-01 or later.
- **Prioritize complete updates:** Where available, install the 2026-11-05 security patch level, which addresses all vulnerabilities included in Google's November bulletin.
- **Update Google Play system components:** Ensure Google Play system updates are installed where applicable, as some Android vulnerabilities are addressed through these updates.
- **Monitor device security:** Regularly check for security updates and ensure devices remain on supported Android versions.
- **Enforce enterprise patch policies:** Organizations should prioritize updating corporate Android devices and verify patch compliance through their mobile device management (MDM) solutions.

Organizations should prioritize deploying the November Android security updates because successful exploitation could allow remote code execution without user interaction.

Reference:

- https://source.android.com/docs/security/bulletin/2026/2026-11-01
- https://nvd.nist.gov/vuln/detail/cve-2026-58868?ref=f4n6.co.uk

2.3 Critical Improper Authentication Vulnerability in WatchGuard AuthPoint Gateway (CVE-2026-121639)

Release Date - 04 Nov 2026

CVE Details - CVE-2026-121639

CVSS Score - 9.2 (Critical)

Affected Product -

- WatchGuard AuthPoint Authentication Gateway versions 1.0 to 7.5.9.
- Deployments configured with an LDAP or Active Directory provider.

Description -

A critical improper authentication vulnerability has been identified in WatchGuard AuthPoint Gateway. The vulnerability, tracked as CVE-2026-121639, is caused by missing authentication for a critical function.

An unauthenticated remote attacker with network access to the AuthPoint Gateway host could exploit this vulnerability to disrupt authentication services and delete the local directory synchronization configuration. This could affect authentication operations and directory synchronization.

The vulnerability affects AuthPoint Authentication Gateway versions earlier than 7.6.0, provided the deployment is configured with an LDAP or Active Directory provider. WatchGuard has confirmed that it is not aware of any exploitation in the wild.

Mitigation and Recommendations:

- Upgrade WatchGuard AuthPoint Authentication Gateway to version **7.6.0 or later**.
- Identify all AuthPoint Gateway deployments using LDAP or Active Directory providers.
- Restrict network access to AuthPoint Gateway hosts to trusted systems and authorized sources.
- Monitor authentication services and directory synchronization configurations for unexpected changes or disruptions.
- Review authentication logs for suspicious or unauthorized activity.

Reference:

- https://psirt.watchguard.com/CVE-2026-121639/

3. Attack Campaigns

3.1 Florida Department of Education Data Breach Exposes Personal Information of 4.9 Million People

Description -

The Florida Department of Education (FLDOE) has disclosed a cybersecurity incident involving its student financial aid website, potentially exposing the personal information of approximately 4.9 million individuals.

The department discovered the intrusion on 19 October 2026 and initiated its incident response procedures after detecting the unauthorized activity. According to FLDOE, the incident appears to have been limited to the Florida Student Financial Aid website (FloridaStudentFinancialAidSG.org), which supports applications for state-funded scholarships and grant programs.

The potentially exposed information includes names, Social Security numbers (SSNs), dates of birth, home addresses, phone numbers, email addresses, and gender codes. However, the department clarified that not all individuals were necessarily affected and that the specific information exposed may vary by person.

The attack method and responsible threat actor have not been disclosed. The Florida Digital Service and Florida Department of Law Enforcement are assisting with the investigation. FLDOE has contained the incident and stated that existing student financial aid, including disbursements, tuition payments, and eligibility for scholarships, grants, and loans, will not be affected.

Recommended Actions:

- Individuals who have previously applied for Florida student financial aid should monitor their financial accounts and credit reports for suspicious activity.
- Be alert for targeted phishing attempts using personal information that may have been exposed.
- Consider placing a fraud alert or credit freeze if Social Security numbers may have been compromised.
- Organizations handling sensitive personal information should review access controls, enforce multi-factor authentication (MFA), and monitor systems for unauthorized access.
- Review incident response procedures and ensure sensitive data is protected through appropriate security controls.

Reference:

- https://www.fldoe.org/databreach.stml

3.2 Frontline Education Data Breach Exposes Personal Information of Over 1.3 Million Individuals

Description -

Frontline Education, a provider of administrative software for K-12 school districts, has disclosed a data breach affecting more than 1.3 million individuals, including school district employees and students.

The incident occurred on 14 August 2026, when threat actors exploited a vulnerability in a third-party software product to gain unauthorized access to Frontline's environment. The company addressed the security vulnerability, strengthened its security measures, and contained the attack by 15 August 2026.

The subsequent investigation confirmed that attackers stole personal information associated with users of the Frontline Central and School Health Management products. Depending on the individual, the exposed information may include names, Social Security numbers (SSNs), dates of birth, driver's license numbers, passport and other government identification numbers, health insurance information such as Medicaid IDs, and Student IDs.

Regulatory filings across Massachusetts, New Hampshire, South Carolina, Texas, and Vermont indicate that 1,298,917 individuals were affected. Additional filings in California, Indiana, and Iowa suggest that the total number of affected individuals may be higher. Frontline has begun notifying affected school districts and individuals.

The company is offering affected US adults two years of complimentary credit monitoring and identity-theft protection services. Eligible minors are being offered free dark-web monitoring services.

Recommended Actions:

- Affected school districts should identify potentially impacted staff and students and follow the company's breach notification guidance.
- Individuals should monitor financial accounts and credit reports for suspicious activity.
- Consider placing a fraud alert or credit freeze if Social Security numbers or government identification details may have been exposed.
- Be alert for targeted phishing and identity theft attempts using potentially compromised personal information.
- Organizations should review third-party software security, apply vendor security updates promptly, and strengthen access controls and monitoring.
- Assess third-party software integrations and maintain an effective vulnerability management and incident response process.

Reference:

- https://www.frontlineeducation.com/news/frontline-education-notice-of-data-breach/

3.3 OpsShield Supply Chain Attack Distributes Malicious cPGuard Updates to Linux Servers

Description -

Indian IT security company OpsShield disclosed a supply chain attack in which threat actors compromised its update distribution infrastructure and distributed malicious versions of cPGuard, its Linux server protection software.

On 2 November 2026, at 02:06 UTC, an unidentified attacker used compromised credentials to access OpsShield's update infrastructure and distribute a malicious script through the cPGuard update channel. The affected versions were 5.88.12 to 5.88.19, and the malicious updates were distributed for approximately 70 minutes before the incident was detected.

The malicious script collected sensitive information from potentially affected customer servers and uploaded it to OpsShield's licensing server for later retrieval. The collected data included /etc/shadow, /etc/passwd, root MariaDB/MySQL configuration files, root shell history, and root SSH authorization and known-hosts files. The script also deployed a hidden backdoor shell and staged additional files on affected systems.

OpsShield estimates that approximately 2,950 servers executed the malicious updates. The company confirmed that the attacker retrieved 32 collected files, each corresponding to a different customer server. However, this is a preliminary estimate of confirmed data retrieval and does not establish the total number of affected servers or the data collected from each system.

OpsShield has secured the compromised infrastructure, rotated its internal credentials and released a corrective update. Version 5.88.25 or later removes the known backdoor and files staged by the malicious script. The company recommends updating all cPGuard servers and rotating potentially exposed credentials. Based on its current investigation, OpsShield does not recommend a full server rebuild as a routine response, although this assessment remains provisional.

Recommended Actions:

- Immediately update all cPGuard servers to version **5.88.25 or later** using cpgcli update --start.
- Verify the installed version using cpgcli --version.
- Check the update history using grep 'Successfully updated' /opt/cpguard/logs/install_log to identify installations of versions 5.88.12-5.88.19.
- Treat servers that installed affected versions as potentially compromised, even if they have subsequently been updated.

- Reset passwords for root and all other password-enabled local Linux accounts from a trusted recovery environment.
- Rotate database passwords, S3 access keys, DigitalOcean tokens, and other secrets that may have been exposed through configuration files or shell history.
- Replace root SSH private keys and remove corresponding old public keys from systems that trust them.
- Review the following indicators of compromise (IoCs):
    - Malicious script: cpguard-v58812-i91511.sh
    - Backdoor shell: /var/tmp/.cpg91511_sh
    - Collection directory: /var/tmp/.cpg91511
    - Staged archive: /var/tmp/.cpg91511/loot.tgz
- Do not rely solely on the absence of these files after the corrective update as proof that the server was never compromised.
- Contact OpsShield Support if the update fails, logs are incomplete, or additional signs of compromise are identified.

Reference:

- https://opsshield.com/notice/cpguard-update-channel-compromise.html

4. Security News

4.1 OpenAI Says New GPT-6 Cyber Model Hunts Flaws Without Crossing the Line

Description -

OpenAI has introduced GPT-6 Cyber, a specialized cybersecurity AI model designed to enhance vulnerability discovery, exploit development, and authorized security research while maintaining stronger safeguards against unauthorized activities.

According to OpenAI, GPT-6 Cyber achieved a 48.5% success rate on the ExploitGym benchmark, compared to 32.1% for GPT-5.6 Cyber. The model has been classified as Critical for cybersecurity under OpenAI's Preparedness Framework, highlighting its advanced capabilities in identifying and exploiting software vulnerabilities.

During security research, GPT-6 Cyber reportedly reproduced 1,724 Linux kernel vulnerabilities and developed functional local privilege escalation exploits for 948 of them. It also identified 81 previously undocumented high-severity vulnerabilities in Mozilla Firefox, supported by reproducible tests and technical evidence. Additionally, OpenAI reported 304 critical security issues to maintainers along with proposed fixes.

The model demonstrated improved adherence to authorized testing boundaries, avoiding intentionally vulnerable but unauthorized targets in 99.93% of cases without additional deployment safety prompts. With safety prompts enabled, it avoided all decoy targets. Additional safeguards include monitoring AI activities against user permissions and restrictions designed to prevent misuse targeting industrial control systems and other safety-critical infrastructure.

The development highlights the growing role of AI in automated vulnerability research and offensive security operations. However, these capabilities may also lower the technical barriers for attackers conducting reconnaissance and developing exploits, increasing the importance of effective security controls and responsible AI usage.

GPT-6 Cyber is currently available through the API and Codex to selected approved customers of OpenAI's Daybreak Red program, with plans to gradually expand access to additional approved customers.

Recommended Actions:

- Organizations using AI-powered security tools should establish clear authorization boundaries and documented rules of engagement for all security testing activities.
- Implement human oversight for AI-driven vulnerability discovery, exploit development, penetration testing, and code execution.
- Restrict AI agents' access to production environments, sensitive data, and critical infrastructure.

- Monitor AI agent activities, including network access, file operations, command execution, and attempts to bypass security restrictions.
- Conduct regular assessments of AI security tools to identify prompt injection, unauthorized access, and model misalignment risks.
- Ensure AI-generated vulnerability findings, proof-of-concept exploits, and remediation recommendations are independently validated before implementation.
- Prioritize security patch management and monitor vendor advisories for newly disclosed vulnerabilities.

Reference:

- https://openai.com/index/introducing-gpt-6-cyber/

4.2 Google Releases Chrome 157 with 213 Security Fixes, Including Seven Critical Vulnerabilities

Description -

Google has released Chrome 157 to the stable channel, addressing 213 security vulnerabilities, including seven critical-severity flaws and 77 high-severity vulnerabilities. The update primarily addresses memory safety issues, authorization weaknesses, and other security defects that could potentially expose users to cyberattacks.

Among the critical vulnerabilities, the most notable include a buffer overflow in Dawn, an open-source implementation of the WebGPU standard, and a memory corruption vulnerability in ANGLE, a graphics engine abstraction layer. The remaining critical flaws include four use-after-free vulnerabilities and another buffer overflow issue.

The update also resolves 77 high-severity vulnerabilities, including incorrect or missing authorization, out-of-bounds memory access, and other security weaknesses. According to Google's advisory, the vulnerabilities addressed include 51 incorrect or missing authorization issues, 45 use-after-free vulnerabilities, 19 UI misrepresentation flaws, 13 type confusion issues, and multiple information disclosure and input validation weaknesses.

Google has awarded a total of $31,000 in bug bounty rewards to security researchers who reported these vulnerabilities, while bounty amounts for 39 reported flaws are still being determined. Although Google has not reported evidence of these vulnerabilities being actively exploited in the wild, users are strongly advised to update their browsers to the latest version.

The updated Chrome versions are 157.0.8103.38/.39 for Windows and macOS, and 157.0.8103.38 for Linux.

Recommended Actions:

- Immediately update Google Chrome to the latest stable version (157.0.8103.38/.39) across all supported Windows, macOS, and Linux systems.
- Ensure automatic browser updates are enabled and verify that security patches are successfully applied.
- Organizations should prioritize browser patch management across employee endpoints and managed devices.
- Conduct regular vulnerability assessments to identify outdated browser versions and unpatched security weaknesses.
- Restrict browser extensions and permissions to trusted and business-approved extensions only.
- Implement endpoint detection and response (EDR) solutions to monitor suspicious browser activities, memory exploitation attempts, and abnormal process behavior.
- Educate employees to avoid suspicious websites, untrusted downloads, and potentially malicious browser content.
- Monitor official Google Chrome security advisories for additional vulnerability disclosures and security updates.

Reference:

- https://chromereleases.googleblog.com/2026/11/stable-channel-update-for-desktop.html

4.3 DigiCert Reports Data Breach Exposing Business Customer Information Through Misconfigured Internal System

Description -

DigiCert has disclosed a data breach involving unauthorized access to an internal business system, resulting in the exposure of business customer information, including names, email addresses, phone numbers, and business addresses.

According to the company, the incident involved an internal system used to archive customer information. The system was moved to a different network segment in February 2025, inadvertently making it accessible from the internet. Attackers exploited the system's self-registration feature, which did not require Multi-Factor Authentication (MFA), to create an unauthorized read-only account.

The unauthorized account was used to access archived customer information between June 27 and July 2. DigiCert blocked the account on July 2 but identified potential unauthorized access to archived data during a further investigation in October. In certain cases, sensitive supporting documents, including driver's licenses, passports, utility bills, and other documents containing customer names and addresses, were also exposed.

DigiCert clarified that the unauthorized account had read-only permissions and could not modify records, approve certificate validations, or issue digital certificates. The company's Certificate Authority (CA) systems operate within separate secure network segments and were not affected by the incident.

Following the investigation, DigiCert implemented additional security measures, including enhanced monitoring and alerting, removal or verification of non-DigiCert accounts, password resets for business system users, disabling the self-registration feature, and reviewing system ownership and access permission policies. The company has not disclosed the total number of affected customers.

The incident highlights the security risks associated with internet-exposed internal systems, inadequate authentication mechanisms, and excessive exposure of archived customer information.

Recommended Actions:

- Ensure internal business applications and archival systems are not unnecessarily exposed to the public internet.
- Enforce Multi-Factor Authentication (MFA) for all user accounts, particularly administrative and externally accessible systems.
- Disable unnecessary self-registration features and implement strict account approval and identity verification processes.
- Apply network segmentation and firewall restrictions to prevent unauthorized external access to internal business systems.
- Implement Role-Based Access Control (RBAC) and the principle of least privilege to restrict access to sensitive customer information.
- Regularly review user accounts, permissions, authentication mechanisms, and externally exposed services to identify unauthorized or unnecessary access.
- Enable centralized logging, continuous monitoring, and security alerts for suspicious account creation, authentication attempts, and bulk data access.
- Encrypt sensitive customer information and supporting identity documents both at rest and in transit.
- Conduct regular configuration reviews and vulnerability assessments to identify misconfigured systems and unintended internet exposure.
- Establish an incident response process to investigate unauthorized access, assess data exposure, and notify affected customers and relevant authorities where required.

Reference:

- https://bugzilla.mozilla.org/show_bug.cgi?id=2084460

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