

Daily Cyber Headlines

Oct 23, 2026

☐ WHITE

[View Alert](#)

Today's Headlines:

Leading Story

- Arista Warns of Critical VeloCloud SQL Injection Zero-Day Exploited in Attacks

Data Breaches & Data Leaks

- Ridgeway Pharmacy Data Breach Affects 259,000 Individuals

Cyber Crimes & Incidents

- SEO Poisoning Campaign Delivers New Armorsteal Malware

Vulnerabilities & Exploits

- Oracle Patches Over 1,200 Vulnerabilities With October 2026 CPU
- Node.js Brotli Decoder Bug Could Allow Remote Code Execution in All Supported Versions

Trends & Reports

- Leveraging Android Intrusion Logs to Expose Advanced Threats
- The Current Landscape of OAuth Attacks

Privacy, Legal & Regulatory

- Nothing To Report

Upcoming Health-ISAC Events

- Global Monthly Threat Brief

- Americas – October 27, 2026, 12:00 PM - 1:00 PM ET
- European – October 28, 2026, 03:00-04:00 PM CET
- APAC – October 30, 2026, 01:00-02:00 PM AEST

Additional Info

Leading Story

[Arista Warns of Critical VeloCloud SQL Injection Zero-Day Exploited in Attacks](#)

Summary

- An actively exploited SQL injection vulnerability, CVE-2026-114625, affects Arista VeloCloud Orchestrator and allows authenticated users with read-only access to gain operator-level privileges. The critical flaw threatens SD-WAN management systems and associated data.

Analysis & Action

Active exploitation of [CVE-2026-114625](#) exposes on-premises VeloCloud Orchestrator deployments to privilege escalation. The vulnerability affects centralized SD-WAN management infrastructure and could compromise administrative control, as well as the confidentiality, integrity, and availability of managed information.

The SQL injection vulnerability carries a CVSS v3.1 score of 9.9 and requires an authenticated session, including Enterprise Read Only access. Successful exploitation enables threat actors to impersonate local superusers and access privileged internal functionality.

Health-ISAC advises members to upgrade affected VeloCloud Orchestrator instances to versions 5.2.3.18, 6.1.3.10, or 6.4.2.12; restrict management interface access; and investigate suspicious web requests, administrative activity, and unexpected outbound connections.

Data Breaches & Data Leaks

[Ridgeway Pharmacy Data Breach Affects 259,000 Individuals](#)

Summary

- Ridgeway Pharmacy disclosed a website-related data breach affecting 258,920 individuals, potentially exposing names, birth dates, prescription details, health and insurance information, and payment card data for some customers. Internal systems were reportedly unaffected.

Analysis & Action

Ridgeway Pharmacy identified the exposure of customer information through a third-party-developed and maintained website. Forensic investigators determined that the incident was confined to the website, highlighting risks associated with externally managed patient-facing platforms.

Exposed information potentially included names, addresses, birth dates, prescription and health information, and insurance details; a subset also had payment card information affected. The available disclosure does not establish the intrusion method or identify a responsible threat actor.

Health-ISAC advises its members to assess security oversight of third-party patient portals, review website access permissions and data storage practices, strengthen monitoring for unauthorized access, and coordinate breach response procedures with external techno

Cyber Crimes & Incidents

[SEO Poisoning Campaign Delivers New Armorsteal Malware](#)

Summary

- Threat actors used poisoned search results and counterfeit Chocolatey and Microsoft Activation Scripts websites to deliver Armorsteal, a Python-based malware family capable of remote command execution, keylogging, screenshot capture, and theft of credentials and cryptocurrency data.

Analysis & Action

The campaign exploited searches for software installation instructions, directing users to impersonation sites that supplied malicious PowerShell commands. These installers also deployed

legitimate software, reducing suspicion while silently establishing persistence on infected Windows systems.

Armorsteal installed a bundled Python runtime under a disguised Windows system directory and persisted through SysCheck2 and SysCheckX scheduled tasks. Its modular payloads collected browser credentials, SSH keys, Discord tokens, clipboard contents, and screenshots.

Health-ISAC advises its members to investigate unusual PowerShell installation commands, identify SysCheck2 and SysCheckX scheduled tasks, inspect suspicious Windows system directories, restrict unauthorized script execution, and review endpoint telemetry for credential theft.

Vulnerabilities & Exploits

[Oracle Patches Over 1,200 Vulnerabilities With October 2026 CPU](#)

Summary

- Oracle released a Critical Patch Update containing 1,295 new security patches that address 1,209 unique CVEs across enterprise products. The release includes 95 critical vulnerabilities, with significant exposure in Fusion Middleware and business applications.

Analysis & Action

Oracle's security update spans databases, middleware, enterprise applications, and other widely deployed platforms. The breadth of affected products underscores the need for coordinated patch management across interconnected business systems and services that support critical operations.

Fusion Middleware received 206 security patches, including 134 vulnerabilities that attackers could exploit remotely without authentication. Additional fixes cover E-Business Suite, Communications, PeopleSoft, MySQL, and Java SE, with risks varying by deployed components and configurations.

Health-ISAC advises its members to inventory Oracle deployments, review product-specific security advisories, prioritize remotely exploitable and critical vulnerabilities, apply supported patches through controlled change processes, and verify remediation across integrated clinical and enterprise systems.

[Node.js Brotli Decoder Bug Could Allow Remote Code Execution in All Supported Versions](#)

Summary

- Node.js released security updates addressing CVE-2026-111497, a high-severity out-of-bounds write in its bundled Brotli decoder that could enable remote code execution when applications decompress malicious data. All supported release lines are affected.

Analysis & Action

Node.js maintainers patched the Brotli decompression weakness alongside nine other vulnerabilities affecting supported runtime branches. Applications that process untrusted compressed requests or fetched responses may be compromised, so assess vulnerable backend services first.

[CVE-2026-111497](#) involves malformed Brotli input triggering an out-of-bounds memory write. Public proof-of-concept testing caused crashes and limited memory disclosure on standard builds but did not demonstrate remote code execution; exploitation in the wild remains unreported.

Health-ISAC advises its members to inventory Node.js services, upgrade to versions 22.23.4, 24.22.1, or 26.12.1 as applicable, migrate unsupported releases, and review applications that decompress untrusted Brotli-encoded requests or external HTTP responses.

Trends & Reports

[The Current Landscape of OAuth Attacks](#)

Summary

- OAuth phishing campaigns increasingly exploit stolen authorization tokens, deceptive consent requests, and malicious redirects to bypass multifactor authentication and retain access to cloud services. Research identifies phishing-as-a-service templates and AI-assisted impersonation as emerging enablers.

Analysis & Action

OAuth abuse shifts the point of compromise from password entry to application authorization, where legitimate sign-ins can grant unintended access. Persistent tokens may remain usable after password resets, complicating account recovery and incident containment.

Observed techniques include device authorization phishing, stolen authorization codes, fraudulent application consent, and manipulated redirect URLs. Obfuscated phishing pages, environment fingerprinting, and reusable templates further complicate detection across interconnected cloud applications.

Health-ISAC advises its members to restrict third-party application consent, require administrative approval for sensitive permissions, audit OAuth redirect URIs, monitor anomalous token activity, and revoke suspicious grants and refresh tokens during incident response.

Privacy, Legal & Regulatory

Nothing to report.

Health-ISAC Cyber Threat Level

On September 17, 2026, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and decided to maintain it at **Yellow (Elevated)**. The Threat Level of **Yellow (Elevated)** is due to threats from:

ShinyHunters Activity, Job Scams, Increase in Vulnerability Reporting, Third-Party Risk, and DPRK IT Worker Fraud.

For more information about the Health-ISAC Cyber Threat Level, including definitions and response guidelines for each of the alert levels, please review the Threat Advisory System.

You must have Cyware Access to reach the Threat Advisory System document. Contact membership@h-isac.org for access to Cyware.

<hr size=1 width="100%" align=center>

Alert Id

f8c46fa8

Category

Daily Cyber Headlines

References

[cyware](#) [securityweek](#) [thehackernews](#) [zscaler](#) [paloaltonetworks](#) [cyware](#)
[1](#) [hipaajournal](#) [thehackernews](#) [1](#)

Tags

OAuth Attacks, Node.js Brotli, Armorsteal, Ridgeway,
VeloCloud, SQL Injection, Oracle

Report Source(s)

Health-ISAC

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Content Powered by BLACKWIRE Labs



Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Please provide your feedback

Like

Dislike

Download the App

Available on iOS, Android and Web



For more updates and alerts, visit: <https://health-isac.cyware.com/webapp/>

Health-ISAC is an invite only platform. Please DO NOT forward this email to anyone. If you are not supposed to receive this email, please report to toc@h-isac.org

--

You received this message because you are subscribed to the Google Groups "TLP Green - Health-ISAC Partners" group.

To unsubscribe from this group and stop receiving emails from it, send an email to health-isac-partners+unsubscribe@h-isac.org.

To view this discussion visit <https://groups.google.com/a/h-isac.org/d/msgid/health-isac-partners/010001a167b9ee7d-438f7aef-3750-4f9e-8fdd-ddd1f67f268f-000000%40email.amazonses.com>.