

SecurityBridge Launches Automated Virtual Patching to Safeguard SAP Systems

New Feature Provides Real-Time Protection for Unpatched SAP Systems, Enhancing Efficiency and Security on SAP Patch Tuesday

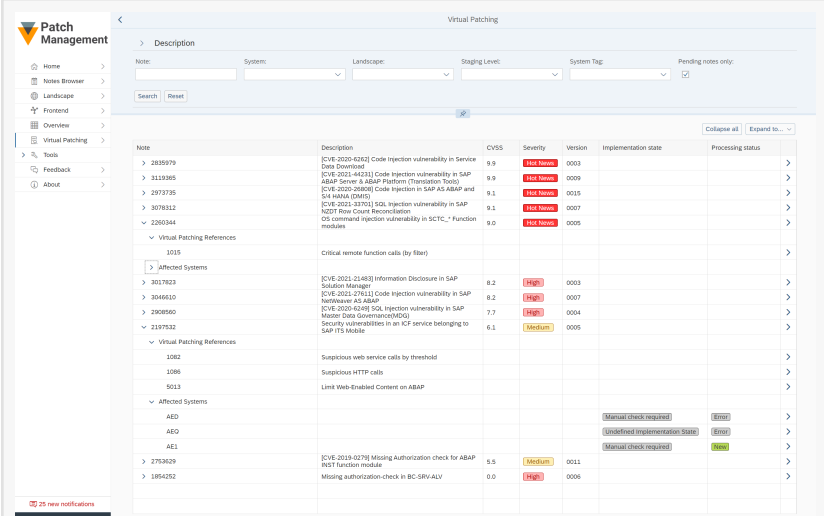
NEW YORK, NY, UNITED STATES, October 24, 2024 /EINPresswire.com/ -- SecurityBridge, the Cybersecurity Command Center for SAP, today announced its latest innovation: [Virtual Patching](#), an advanced feature that enhances SAP security by providing automated protection for unpatched SAP systems starting on SAP Patch Day.

Virtual Patching is a cross-platform solution that integrates SecurityBridge's Patch Management and Threat Detection modules. It offers seamless, real-time defense against vulnerabilities by alerting SAP administrators when unpatched code is detected. The solution protects affected SAP systems until official patches are implemented, allowing administrators to follow their patch management processes without compromising security.

“Our cross-functional innovation in Virtual Patching underscores SecurityBridge's leadership in SAP security,” said Holger Hugel, Product Management Director at SecurityBridge. “With this 100 percent automated approach, SAP systems are safeguarded from the first moment a vulnerability is disclosed, ensuring continuous protection.”

Addition features of SecurityBridge's Virtual Patching include:

-Automated Threat Detection: Alerts are generated only for impacted SAP systems, ensuring targeted and relevant notifications.



The screenshot displays the 'Patch Management' interface with a 'Virtual Patching' section. It features a table of vulnerabilities with columns for Note, Description, CVSS, Severity, Version, Implementation date, and Processing status. The table lists several CVEs with their respective severity levels (High, Medium) and implementation dates. A notification bar at the bottom indicates '25 new notifications'.

| Note | Description | CVSS | Severity | Version | Implementation date | Processing status |
|-----------------------------|---|------|----------|---------|----------------------------------|-------------------|
| 2839979 | [CVE-2024-4242] Code injection vulnerability in Service Data Download | 9.9 | High | 0003 | | |
| 3118395 | [CVE-2024-4421] Code injection vulnerability in SAP ABAP Server & ABAP Platform (Transaction Tools) | 9.9 | High | 0009 | | |
| 2973725 | [CVE-2024-3796] Code injection in SAP AS ABAP and S4 HANA (DMS) | 9.1 | High | 0015 | | |
| 3076612 | [CVE-2024-3275] SQL injection vulnerability in SAP NZDT Row Count Recalculation | 9.1 | High | 0007 | | |
| 2265344 | [CVE-2024-3275] SQL injection vulnerability in SCITC - Function modules | 9.0 | High | 0005 | | |
| Virtual Patching References | | | | | | |
| 1015 | Critical remote function calls (by file) | | | | | |
| Affected Systems | | | | | | |
| 3017823 | [CVE-2024-2148] Information Disclosure in SAP Solution Manager | 8.2 | High | 0003 | | |
| 3046610 | [CVE-2024-2761] Code injection vulnerability in SAP NetWeaver AS ABAP | 8.2 | High | 0007 | | |
| 2908560 | [CVE-2024-4240] SQL injection vulnerability in SAP Master Data Governance (MDG) | 7.7 | High | 0004 | | |
| 2197532 | Security vulnerabilities in an ICF service belonging to SAP ITx Mobile | 6.1 | Medium | 0005 | | |
| Virtual Patching References | | | | | | |
| 1082 | Suspicious web service calls by threshold | | | | | |
| 1086 | Suspicious HTTP calls | | | | | |
| 5013 | Link Web-Enabled Content on ABAP | | | | | |
| Affected Systems | | | | | | |
| 4E0 | | | | | (Manual check required) | Error |
| 4E0 | | | | | (Unpatched implementation state) | Error |
| 4E1 | | | | | (Manual check required) | |
| 1730320 | [CVE-2019-0276] Missing Authorization check for ABAP NFS function module | 5.8 | Medium | 0011 | | |
| 1854252 | Missing authorization check in BC-SRPAALV | 0.0 | High | 0006 | | |

Virtual Patching connects information from SAP Security Notes with the security signatures, allowing customers to see which monitoring listener or vulnerability check will provide that compensating control until the corresponding patch is implemented.

-Pre-configured Signatures: SecurityBridge updates its Threat Detection signatures via the cloud, requiring no manual system updates.

-Patch Day Protection: SAP systems are automatically shielded from vulnerabilities when new SAP SecurityNotes are released on Patch Tuesday.

With the release of version 6.30 in early October 2024, Virtual Patching is now included in the SecurityBridge Platform subscription, making it a crucial tool for enterprises looking to streamline their SAP security operations.

About SecurityBridge, Inc.

SecurityBridge is the leading provider of a comprehensive, SAP-native cybersecurity platform. Trusted by organizations worldwide to safeguard their most critical business systems, our platform seamlessly integrates real-time threat monitoring, vulnerability management, and compliance capabilities directly into the SAP environment, empowering organizations to protect their data's integrity, confidentiality, and availability with minimal manual effort. With a proven track record, including a stellar customer success rating and over 5,000 SAP systems secured globally. SecurityBridge stands out for its ability to accurately provide a 360° view of the SAP security posture, ease of use, rapid implementation, and transparent licensing. We are committed to innovation, transparency, and customer-centricity, ensuring businesses can confidently navigate the evolving landscape of SAP security threats. For more information, visit www.securitybridge.com.

###

Source: [BridgeView Marketing PR Services](#)

Betsey Rogers

Bridgeview Marketing

betsey@bridgeviewmarketing.com

Visit us on social media:

[X](#)

[LinkedIn](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/754248748>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2024 Newsmatics Inc. All Right Reserved.