INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-14 06:04 UTC

SAP March 2026 Patch Day: Critical SQL Injection, DoS, and Code Injection Vulnerabilities Addressed

SECURITY ANALYSIS | CRITICAL | CVSS 9.0

SCC Item ID	SCC-STY-2026-0059
Type	Security Analysis
Severity	CRITICAL
CVSS Base Score	9.0
Affected Products	Multiple SAP products (specific product-version mappings require verification against SAP Security Notes on SAP Support Portal, March 2026 Patch Day)
Published	24 minutes ago
Discovery Source	Serper

Executive Summary

SAP's March 2026 Patch Day addressed 15 security notes, including two rated critical, covering SQL injection, denial-of-service, and code injection vulnerabilities across multiple SAP product lines. Organizations running unpatched SAP environments face exposure to unauthorized database access, application disruption, and arbitrary code execution, risks that are especially acute given SAP's prevalence in enterprise ERP, finance, and supply chain operations. The patch cycle reinforces a consistent pattern: SAP environments remain high-value targets, and delayed patching in complex enterprise deployments continues to widen the window of exploitation.

Technical Analysis

SAP's March 2026 Security Patch Day released 15 Security Notes, two of which carried critical severity ratings. The disclosed vulnerability classes map directly to three weakness categories: CWE-89 (SQL Injection), CWE-400 (Uncontrolled Resource Consumption), and CWE-94 (Code Injection). These weaknesses correspond to MITRE ATT&CK techniques T1190 (Exploit Public-Facing Application), T1059 (Command and Scripting Interpreter), and T1499 (Endpoint Denial of Service).

SQL injection flaws (CWE-89) in SAP applications represent a particularly high-impact class. SAP systems routinely process sensitive business data, financial records, HR data, supply chain configurations, and a successful SQLi exploit against an internet-facing or internally accessible SAP application could yield unauthorized read or write access to underlying databases without authentication. The MITRE T1190 mapping

is direct: threat actors targeting enterprise ERP platforms frequently probe for known unpatched vulnerabilities in SAP NetWeaver and related components, as documented in prior Onapsis and CISA advisories.

Code injection vulnerabilities (CWE-94, T1059) raise the severity profile further. If an attacker can inject and execute arbitrary code within an SAP application context, lateral movement into connected systems becomes a viable follow-on objective. SAP landscapes are often deeply integrated with Active Directory, financial backends, and third-party logistics platforms, expanding the impact surface if a compromise occurs. Denial-of-service vulnerabilities (CWE-400, T1499) carry a different risk profile: even without data exfiltration, disrupting SAP availability in manufacturing, logistics, or financial environments can trigger direct operational and revenue impact.

Specific CVE identifiers, affected product-version mappings, and CVSS scores are documented in SAP Security Notes published on the SAP Support Portal for March 2026. Onapsis and RedRays have historically provided corroborating technical analysis of SAP patch cycles and are recommended reference points for teams performing triage. Per RedRays' LinkedIn post referencing the March 2026 cycle, 15 notes were released with two critical designations. Note: precise CVE numbers and affected product versions require direct validation against the SAP Support Portal Security Notes, as the source article (CyberPress) is a T3 news aggregator without primary source documentation.

The qualitative CVSS estimate of 9.0 in the item data reflects the critical classification but is not a formally published vendor CVSS score, teams should pull authoritative scores directly from the SAP Support Portal before using this figure in risk calculations.

Action Checklist

1. Step 1: Assess exposure, identify all SAP products and versions deployed in your environment (SAP NetWeaver, S/4HANA, Business One, BusinessObjects, and others); cross-reference against the March 2026 SAP Security Notes on the SAP Support Portal at support.sap.com to confirm which specific notes apply to your deployment
2. Step 2: Prioritize the two critical notes first; navigate to the SAP Support Portal (support.sap.com > My Support > Security Notes News > March 2026 Patch Day), identify and download the two notes rated critical, and fast-track patching for affected products; do not rely on third-party summaries alone, validate CVSS scores and affected versions from the official SAP source
3. Step 3: Review controls for SQLi and code injection exposure, confirm web application firewall (WAF) rules are active and tuned for SAP-specific SQLi patterns; verify that SAP application servers are not directly internet-facing without authentication controls; audit SAP user authorization models for least-privilege compliance
4. Step 4: Assess DoS resilience, review rate limiting, resource quotas, and availability monitoring for SAP application tiers; confirm that SAP system availability is covered in your incident response and business continuity plans, particularly for ERP-dependent operations (finance close cycles, manufacturing, logistics)
5. Step 5: Update threat model, add CWE-89/CWE-94 exploitation of SAP applications as an active risk scenario; reference MITRE T1190 (Exploit Public-Facing Application) and T1059 (Command and Scripting Interpreter) in your threat register with SAP as a named affected asset class
6. Step 6: Communicate findings, brief application owners and business unit leads on patching timelines; frame risk in operational terms (ERP downtime, financial data exposure) rather than technical jargon; document patch status for compliance and audit purposes

7. Step 7: Monitor for follow-up disclosures, track Onapsis (onapsis.com/blog) and RedRays for detailed technical analysis of the March 2026 notes; watch for proof-of-concept exploit publication, which historically accelerates exploitation timelines for SAP vulnerabilities

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and activate the IR plan immediately if SAP Security Audit Log (SM20) shows AU1 events (ABAP report creation) by non-developer accounts, anomalous S_DEVELOP or SAP_ALL authorization grants, or ICM access logs show SQLi payload patterns against OData/RFC-over-HTTP endpoints — any of these indicate active exploitation of the March 2026 CWE-89/CWE-94 vulnerabilities, which in SAP ERP environments creates regulatory escalation obligations under SOX (financial data integrity), GDPR/CCPA (customer PII in SAP HR/CRM modules), and HIPAA (if SAP is used in healthcare supply chain or billing workflows).
Recovery Notes	After patching, verify remediation by re-running SAP's Security Optimization Service (SOS) report against patched systems and confirming the specific March 2026 Security Notes no longer appear as open findings; simultaneously run a full SAP Security Audit Log review (SM20) for the patch maintenance window to detect any unauthorized ABAP program creation, user master changes, or RFC executions that may indicate exploitation occurred during the vulnerability exposure period. Monitor SAP application server work process utilization (SM50/SM66), ICM connection counts, and enqueue server queue depth (SM12) for 14 days post-patch as a baseline re-establishment period, given that DoS-class vulnerabilities in this patch cycle may have been used to mask concurrent SQLi or code injection activity. Retain all SAP Security Audit Logs, ICM access logs, and system change logs from the 90-day pre-patch window for a minimum of 12 months in write-protected storage to support any retroactive forensic investigation or regulatory inquiry.

Forensic Artifacts	SAP Security Audit Log (transaction SM20/SM21): Filter for event classes AU (ABAP/user changes), DU (authorization failures), and RH (HTTP security events) — CWE-94 code injection exploits against SAP NetWeaver/S/4HANA leave AU1 (ABAP report created) and AU7 (sensitive transaction executed) entries by unexpected user accounts or RFC service users | SAP ICM access log (file path: /usr/sap//D/work/dev_icm and dev_icm_sec): Contains raw HTTP request logs including URIs, source IPs, and HTTP methods — CWE-89 SQLi exploitation attempts against SAP OData services (/sap/opu/odata/) or SOAP endpoints (/sap/bc/srt/) will appear as malformed POST requests with SQL metacharacters in query parameters or request bodies | SAP Web Dispatcher access and error logs (sapmnt//sys/global/wdisp/ or configured log directory): Captures all inbound HTTP/HTTPS traffic before it reaches the application server — DoS exploitation targeting the March 2026 vulnerabilities will manifest as connection exhaustion events (HTTP 503 spikes, max_conn threshold alerts) correlated with specific source IP ranges or URI patterns | ABAP program directory and transport logs (transaction SE09/SE10 and file system path /usr/sap/trans/): Unauthorized ABAP object creation or modification resulting from CWE-94 code injection will generate transport request entries with creation timestamps and user IDs inconsistent with authorized change management windows — cross-reference with change management system (SAP ChaRM or external ITSM) for unmatched entries | SAP syslog and work process trace files (/usr/sap//D/work/dev_w* and dev_disp): Capture low-level application crashes, RFC communication errors, and OS-level command execution traces — exploitation of code injection vulnerabilities via ABAP OS command execution (CALL 'SYSTEM' or SXPG_CALL_SYSTEM function module abuse) will generate entries in work process traces and operating system audit logs (Linux auditd or Windows Security Event Log Event ID 4688 for child processes spawned by the SAP work process executable `disp+work`)

Per-Action IR Details

Step 1: Assess exposure — identify all SAP products and versions deployed in your environment (SAP NetWeaver, S/4HANA, Business One, BusinessObjects, and others); cross-reference against the March 2026 SAP Security Notes on the SAP Support Portal at support.sap.com to confirm which specific notes apply to your deployment

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR Capability and Asset Visibility

Controls: NIST SI-2 (Flaw Remediation), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST RA-5 (Vulnerability Monitoring and Scanning), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: If no CMDB exists, run a network scan with nmap targeting SAP default ports (3200-3299 for DIAG/RFC, 8000/8443 for ICM HTTP/HTTPS, 4300 for Message Server, 50000-50099 for SAP Web Dispatcher) to enumerate live SAP instances: `nmap -sV -p 3200-3299,8000,8443,4300,50000-50099 -oN sap_inventory.txt`. Cross-reference output against SAP system landscape documentation (transaction SMSY or RZ70 output if accessible) to build a version map before pulling Security Notes.

Evidence: Before performing inventory, snapshot the current SAP system landscape directory (SLD) export or LMDB content if available — this establishes a baseline of deployed SAP components and versions (product name, SP level, kernel patch level) at the time of advisory receipt, which is critical for post-patch compliance attestation. Capture SAP kernel version from each system using `disp+work -version` or transaction SM51 output.

Step 2: Prioritize the two critical notes first — pull the SAP Security Notes for March 2026, identify the two notes rated critical, and fast-track patching for affected products; do not rely on third-party summaries alone — validate CVSS scores and affected versions from the official SAP Support Portal

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Prioritization Criteria and Patch Readiness

Controls: NIST SI-2 (Flaw Remediation), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST RA-3 (Risk Assessment), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: For teams without a vulnerability management platform, use SAP's built-in Security Optimization Service (SOS) report (transaction RSECNOTE or the SAP Solution Manager patch analytics dashboard) to identify which installed components are affected by specific Security Notes. If Solution Manager is unavailable, manually query the SAP Support Portal note search filtered by 'March 2026' and 'Priority: HotNews/Critical' and record Note numbers, CVSS base scores, and affected component/version ranges in a tracking spreadsheet. Stage patches in a non-production SAP client before production deployment.

Evidence: Before applying patches, capture a full SAP system configuration baseline: export ABAP program checksums via transaction SE38 for any programs referenced in the critical Security Notes, capture current ICM (Internet Communication Manager) configuration via transaction SMICM (active services and handlers), and record the output of transaction SUIM for privileged user assignments. This baseline detects any pre-existing exploitation of the SQLi or code injection vulnerabilities (e.g., unauthorized ABAP report creation or modified ICM handlers) before patches obscure the evidence.

Step 3: Review controls for SQLi and code injection exposure — confirm web application firewall (WAF) rules are active and tuned for SAP-specific SQLi patterns; verify that SAP application servers are not directly internet-facing without authentication controls; audit SAP user authorization models for least-privilege compliance

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: Short-Term Containment and System Isolation

Controls: NIST AC-3 (Access Enforcement), NIST AC-17 (Remote Access), NIST SC-7 (Boundary Protection), NIST SI-10 (Information Input Validation), NIST SI-4 (System Monitoring), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: For teams without a commercial WAF, deploy ModSecurity with the OWASP Core Rule Set (CRS) in front of SAP Web Dispatcher or ICM, and add SAP-specific rules blocking SQL metacharacter injection into SAP OData and RFC-over-HTTP endpoints (URI patterns containing `%27`, `--`, `UNION SELECT`, `EXEC`, `xp_`, and SAP-specific function module names in query strings). Audit SAP authorization objects S_RFC, S_TCODE, and S_DEVELOP using transaction SU53 failed authorization logs and SUIM role analysis — flag any non-basis users holding S_DEVELOP with DEVCLASS `*` or S_RFC with ACTVT 16 (execute all).

Evidence: Collect SAP ICM access logs (default path: `/usr/sap//D/work/dev_icm`) and SAP Web Dispatcher access logs for HTTP requests containing SQL injection payloads or anomalous ABAP function module invocation patterns in OData service URIs. Capture SAP Security Audit Log (transaction SM20) filtered for event class DU (authorization failures) and AU (user master changes) in the 30 days preceding the advisory — SQLi exploitation attempts against SAP NetWeaver often precede privilege escalation via SAP_ALL or S_DEVELOP authorization grants.

Step 4: Assess DoS resilience — review rate limiting, resource quotas, and availability monitoring for SAP application tiers; confirm that SAP system availability is covered in your incident response and business continuity plans, particularly for ERP-dependent operations (finance close cycles, manufacturing, logistics)

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: IR Plan Coverage and Business Continuity Alignment

Controls: NIST CP-2 (Contingency Plan), NIST CP-10 (System Recovery and Reconstitution), NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SC-5 (Denial-of-Service Protection), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Use SAP transaction SM50 (Work Process Overview) and SM66 (Global Work Process Overview) to establish normal baseline work process utilization; configure SAP CCMS alert monitors (transaction RZ20) with thresholds for work process saturation (>80% DIALOG processes occupied) and enqueue server overload — these are the primary impact indicators for DoS conditions targeting SAP application servers. For network-layer DoS, configure

rate limiting on the SAP Web Dispatcher (`wdisp/max_conn` parameter) and ICM (`icm/max_conn`, `icm/req_queue_len`) and document baseline values before any attack occurs.

Evidence: Before a DoS event occurs, export current SAP system performance baselines from transaction ST05 (SQL Trace), SM04 (User Sessions), and AL08 (All Users Logged On) — these establish normal concurrency levels and query patterns, making it possible to distinguish DoS exploitation of the March 2026 vulnerabilities from organic load spikes. Also capture SAP enqueue server statistics (transaction SM12) and RFC server group configurations (transaction RZ12) as a baseline for post-incident comparison.

Step 5: Update threat model — add CWE-89/CWE-94 exploitation of SAP applications as an active risk scenario; reference MITRE T1190 (Exploit Public-Facing Application) and T1059 (Command and Scripting Interpreter) in your threat register with SAP as a named affected asset class

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Threat Intelligence Integration and Attack Vector Characterization

Controls: NIST RA-3 (Risk Assessment), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST IR-4 (Incident Handling), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Develop Sigma detection rules targeting SAP ICM access logs for T1190 indicators: HTTP POST requests to SAP OData endpoints (`/sap/opu/odata/`) or SOAP/RFC-over-HTTP endpoints (`/sap/bc/`) containing SQL metacharacters or ABAP OS command injection strings (e.g., backtick, `CALL 'SYSTEM'`, `OPEN DATASET`). For T1059 (ABAP as a scripting interpreter), monitor SAP Security Audit Log (SM20) for event AU1 (ABAP program creation) and AU7 (transaction starts for SE38/SA38/SE80) by non-developer users — this is the forensic signature of CWE-94 code injection exploitation in SAP environments.

Evidence: Pull the SAP Security Audit Log (SM20/SM21) for the 90 days preceding this advisory and search for: (1) AU1 events (ABAP report created/modified) by users not in authorized developer roles, (2) transaction SE38 or SA38 execution by basis/RFC service accounts, and (3) failed RFC calls (event class RF) to sensitive function modules (RFC_READ_TABLE, SUSR_USER_CHANGE_PASSWORD_RFC, SXPG_CALL_SYSTEM) — these are the post-exploitation indicators for both the CWE-89 SQLi and CWE-94 code injection classes addressed in the March 2026 notes.

Step 6: Communicate findings — brief application owners and business unit leads on patching timelines; frame risk in operational terms (ERP downtime, financial data exposure) rather than technical jargon; document patch status for compliance and audit purposes

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Lessons Learned, Documentation, and Stakeholder Communication

Controls: NIST IR-6 (Incident Reporting), NIST IR-8 (Incident Response Plan), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-11 (Audit Record Retention), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Maintain a SAP Security Note remediation tracking register (spreadsheet or ticketing system) recording: Note number, vulnerability class (SQLi/DoS/Code Injection), affected SAP product and version, CVSS score, patch applied date, applied-by user, and pre/post-patch system verification result from transaction SNOTE. For compliance documentation, export SAP System Recommendations report from Solution Manager or the SNOTE correction status per system — this serves as audit evidence of patch deployment for SOX IT General Controls or ISO 27001 Annex A.8.8 (Management of technical vulnerabilities) audits.

Evidence: Before closing patching tickets, capture post-patch ABAP correction log exports (transaction SNOTE → 'Correction Status' report) and the SAP kernel version string (`disp+work -version`) for each patched system as immutable compliance artifacts. Also export a post-patch SUIM authorization audit snapshot to confirm no new S_DEVELOP or S_RFC wildcard grants were introduced during the patching maintenance window — a known risk when basis teams apply transport requests under time pressure.

Step 7: Monitor for follow-up disclosures — track Onapsis (onapsis.com/blog) and RedRays for detailed technical analysis of the March 2026 notes; watch for proof-of-concept exploit publication, which historically accelerates exploitation timelines for SAP vulnerabilities

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Threat Intelligence Integration and Indicator Monitoring

Controls: NIST SI-5 (Security Alerts, Advisories, and Directives), NIST SI-4 (System Monitoring), NIST IR-4 (Incident Handling), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Configure free RSS/Atom feed monitoring (using a tool such as RSS-Bridge or a simple cron job with curl + grep) for Onapsis Research Labs blog and RedRays advisory feed, alerting on keywords matching the March 2026 SAP Note numbers. Once PoC indicators emerge, immediately deploy YARA rules scanning SAP application server working directories (`/usr/sap//D/work/`) for newly created ABAP load files (`.ENQ`, `.LOAD` extensions) with timestamps post-advisory — anomalous ABAP load creation is a primary indicator of CWE-94 code injection exploitation. Additionally, set up osquery on SAP application servers to monitor for new file creation in ABAP program directories with a 15-minute poll interval.

Evidence: When PoC publication is detected, immediately pull a fresh SAP Security Audit Log (SM20) snapshot filtered for the 48 hours preceding and following PoC publication, specifically hunting for: AU1 (ABAP created), DU2 (authorization check failures on RFC), and RH (HTTP security events from ICM). Cross-reference with SAP Web Dispatcher/ICM access logs for spikes in POST requests to SAP OData or SOAP endpoints — historically, SAP exploitation accelerates within 24-72 hours of PoC availability, and this log window captures the earliest exploitation attempts against unpatched systems.

Detection Guidance

Detection for this patch cycle should focus on three behavioral themes aligned to the disclosed vulnerability classes.

For SQL injection (CWE-89, T1190): Review SAP application server logs and any WAF or reverse proxy logs for anomalous query strings targeting SAP endpoints, look for patterns consistent with SQLi payloads (UNION SELECT, stacked queries, blind injection timing anomalies). SAP Security Audit Log (transaction SM20, accessible via SAP GUI) and system logs (SM21) should be checked for unexpected RFC calls or database access from non-standard users or service accounts. Onapsis has documented SAP-specific SQLi detection patterns in prior research.

For code injection (CWE-94, T1059): Monitor for unexpected process execution originating from SAP application server processes (e.g., unusual child processes spawned by SAP work processes on Windows or unexpected shell executions on Linux hosts). SAP ABAP runtime error logs and system change logs may surface unexpected code execution events. EDR telemetry on SAP application servers should be reviewed for anomalous process trees.

For denial-of-service (CWE-400, T1499): Baseline SAP system resource utilization (CPU, memory, work process queue depth via transaction SM50/SM66) and alert on deviations. Monitor for unusual spikes in inbound connection volume to SAP message servers or application servers, which may indicate resource exhaustion attempts.

General: Ensure SAP Solution Manager or equivalent monitoring captures availability and performance anomalies in near-real-time. If your organization uses Onapsis Defend or a similar SAP-specific security monitoring tool, verify signature updates have been applied for the March 2026 vulnerability classes.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`Pending — refer to SAP Support Portal March 2026 Security Notes (support.sap.com/en/my-support/knowledge-base/security-notes-news/march-2026.html)`	Specific CVE identifiers, affected product-version mappings, and authoritative CVSS scores for the 15 March 2026 Security Notes, including the two critical-rated notes, are published directly in SAP Security Notes on the SAP Support Portal — access requires an SAP S-user account	LOW
URL	`Pending — refer to Onapsis blog (onapsis.com/blog) for March 2026 SAP patch day analysis`	Onapsis historically publishes detailed technical breakdowns of SAP patch cycles including affected components, exploitation complexity assessments, and detection guidance — March 2026 analysis expected post-patch-day	LOW

Framework Mappings

MITRE-ATTACK

- **T1059** — Command and Scripting Interpreter
- **T1190** — Exploit Public-Facing Application
- **T1499** — Endpoint Denial of Service

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SC-5** — Denial-of-Service Protection
- **SI-10** — Information Input Validation

OWASP-TOP10-2021

- **A03:2021** — Injection

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **13.8** — Deploy a Network Intrusion Prevention Solution

- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.8.8** — Management of technical vulnerabilities
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1059	Command and Scripting Interpreter	Execution
T1190	Exploit Public-Facing Application	Initial-Access
T1499	Endpoint Denial of Service	Impact

Sources

Source	URL	Tier
	https://cyberpress.org/sap-patch-day-fixes-critical-sql-injection-d...	T3
SAP Security Patch Day - January 2026 - SAP Support Portal	https://support.sap.com/en/my-support/knowledge-base/security-notes...	T3
SAP Security Notes: February 2026 Patch Day - Onapsis	https://onapsis.com/blog/sap-security-notes-february-2026-patch-day/	T3
SAP Security Patch Day - March 2026 - SAP Support Portal	https://support.sap.com/en/my-support/knowledge-base/security-notes...	T3
SAP Security Patch Day: 15 Notes, 2 Critical, Patch Now | RedRays	https://www.linkedin.com/posts/redrays_sap-security-patch-day-march...	T3

Generated 2026-04-14 06:04 UTC by TJS Security Command Center