INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-12 14:09 UTC

Microsoft SSO Plugin for Jira & Confluence Elevation of Privilege Vulnerability (CVE-2026-41103)

CVE VULNERABILITY | CRITICAL | CVSS 9.1

SCC Item ID	SCC-CVE-2026-0160
Type	CVE Vulnerability
CVE ID	CVE-2026-41103
Severity	CRITICAL
CVSS Base Score	9.1
Affected Products	Microsoft SSO Plugin for Jira and Confluence (SAML SSO plugin); specific affected versions not confirmed from available source data
Published	2026-05-12T07:00:00
Discovery Source	Msrc Patch Tuesday

Executive Summary

A critical privilege escalation vulnerability (CVE-2026-41103, CVSS 9.1) has been disclosed in Microsoft's SAML SSO plugin for Atlassian Jira and Confluence, released as part of Microsoft's May 2026 Patch Tuesday. Organizations using this plugin allow Microsoft identity credentials to control access to project management and collaboration platforms; a successful exploit could allow an attacker to elevate their privileges within those environments without authorization. Organizations should monitor the MSRC advisory for patch availability and treat this as a priority remediation item given the critical CVSS score and the sensitive nature of Jira and Confluence data in most enterprise environments.

Technical Analysis

CVE-2026-41103 is an Elevation of Privilege (EoP) vulnerability in Microsoft's SAML-based SSO plugin for Atlassian Jira and Confluence. CVSS base score: 9.1 (from vendor/MSRC; NVD score pending). Disclosed via Microsoft Security Response Center (MSRC) as part of the May 2026 Patch Tuesday release cycle. MITRE ATT&CK mappings indicate Valid Accounts (T1078) and Pass the Token (T1550.001) as likely attack techniques based on the EoP classification, though specific exploitation paths have not been published. Specific affected plugin version ranges, the technical root cause, and a confirmed exploitation mechanism have not been published in available source data at analysis time. No CWE identifiers are currently assigned; likely candidates include CWE-269 (Improper Access Control) pending formal NVD assessment. EPSS score is 0.0 (not yet

modeled), and the vulnerability is not listed on CISA's Known Exploited Vulnerabilities catalog as of the configuration date. Patch availability and version guidance should be obtained directly from the MSRC advisory at https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41103 and cross-referenced with Atlassian's official plugin update channels. This analysis was conducted on the configuration date (2026-03-04); version and patch information may be available in the published MSRC advisory, verify before deploying mitigations. Note: Treat all deployments as potentially affected until vendor guidance clarifies version scope.

Action Checklist

1. Step 1: Containment, Identify all instances of the Microsoft SAML SSO plugin deployed across Jira and Confluence environments. Monitor the MSRC advisory (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41103) for patch availability. Once a patched version is released, stage the update immediately. Where patching cannot occur within 24 hours, consider temporarily restricting SSO-authenticated access to Jira and Confluence and requiring fallback to local authentication for privileged accounts until the patch is applied.
2. Step 2: Detection, Query Jira and Confluence access logs for anomalous privilege changes, unexpected role assignments, or administrative actions performed by non-admin accounts authenticated via SAML SSO. Review Azure AD / Entra ID sign-in logs for SAML token issuance anomalies, unexpected assertion targets, or authentication events outside normal user behavior baselines. MITRE T1078 and T1550.001 suggest looking for reuse of authentication tokens across sessions or accounts that authenticated once and then accessed resources inconsistent with their role.
3. Step 3: Eradication, Once Microsoft publishes the patched version number and release mechanism in the May 2026 Patch Tuesday guidance, apply the update as directed by MSRC and Atlassian. If patched versions are not immediately available, contact MSRC and Atlassian support directly for interim guidance. After patching, invalidate all active SAML sessions for Jira and Confluence and require re-authentication. Revoke any suspicious tokens identified during detection review.
4. Step 4: Recovery, After applying the patch, validate that SAML SSO authentication flows are functioning correctly and that no privilege assignments made during the exposure window persist. Audit current role assignments in Jira and Confluence against your authoritative identity directory. Monitor authentication and privilege-change logs for 72 hours post-remediation for residual anomalies.
5. Step 5: Post-Incident, Review your plugin update management process; third-party SSO plugins integrated with enterprise collaboration platforms should be included in patch prioritization workflows, not treated as set-and-forget integrations. Evaluate whether SAML assertion validation controls are logged and monitored in your SIEM. Map this event to NIST CSF PR.AC-1 (identity management) and DE.AE-2 (anomaly detection) as a control gap reference point.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal/compliance immediately if the Jira/Confluence audit log diff reveals any unauthorized privilege escalation events affecting projects or spaces containing PII, PHI, PCI-scoped data, or regulated intellectual property, as this converts the vulnerability event into a reportable data access incident under applicable breach notification frameworks (GDPR Article 33, HIPAA §164.400, state breach notification statutes).

Recovery Notes	After patching the Microsoft SAML SSO plugin and invalidating all SAML sessions, re-validate every Jira project role and Confluence space permission for accounts that authenticated via SAML SSO during the exposure window, comparing against your Entra ID group membership as the authoritative source — do not assume pre-patch permission states were legitimate. Monitor Jira and Confluence audit logs and Entra ID sign-in logs continuously for the 72-hour post-remediation window, specifically alerting on any new privilege assignments to SAML-authenticated accounts or any administrative actions from IP addresses associated with suspicious sessions identified during detection. If your Jira or Confluence instances are externally accessible, consider temporarily enforcing Conditional Access policies in Entra ID requiring compliant devices or named locations for the Jira/Confluence enterprise app registrations during the monitoring window.
Forensic Artifacts	Atlassian Jira audit log (/log/atlassian-jira.log and Administration > System > Audit Log export): Filter for 'addUserToRole', 'grantAdminPermission', 'updateGroupMembership' events where the authenticated user's session was established via SAML SSO — these are the direct forensic signature of CVE-2026-41103 privilege escalation execution. | Atlassian Confluence audit log (/logs/atlassian-confluence.log and Administration > General Configuration > Audit Log): Filter for space permission grants, admin group additions, or anonymous access enablement events tied to SAML-authenticated sessions during the exposure window. | Microsoft Entra ID (Azure AD) Sign-in logs for the Jira and Confluence enterprise application registrations: Export via MS Graph API (GET /auditLogs/signIns?$filter=appId eq '') and inspect for SAML token issuances with anomalous NameID values, unexpected Recipient/Audience attributes in assertions, or authentication from IP addresses outside baseline geographies — these indicate SAML assertion manipulation consistent with the CVE-2026-41103 attack vector. | Web server access logs for the Atlassian application server (Apache/Nginx/Tomcat access logs): Filter for repeated POST requests to the SAML Assertion Consumer Service endpoint (/plugins/servlet/saml/auth) originating from a single IP or user agent in rapid succession — SAML token replay or forged assertion submission would produce this pattern. | Installed plugin file system artifact: The vulnerable Microsoft SAML SSO plugin .jar or .obr file in /plugins/installed-plugins/ or /confluence/WEB-INF/atlassian-bundled-plugins/ — preserve the exact file with its SHA-256 hash as proof of the affected version and to enable vendor-assisted forensic analysis of the specific vulnerability class present in that build.

Per-Action IR Details

Step 1: Containment — Identify all instances of the Microsoft SAML SSO plugin deployed across Jira and Confluence environments. If an updated plugin version is available via the MSRC advisory (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41103), stage the update immediately. Where patching cannot occur within 24 hours, consider temporarily restricting SSO-authenticated access to Jira and Confluence and requiring fallback to local authentication for privileged accounts until the patch is applied.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), NIST AC-2 (Account Management), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Use the Atlassian marketplace admin console (Jira: Administration > Manage apps; Confluence: Administration > Find new apps) to enumerate all installed plugin versions across every node in your deployment — for Data Center deployments this must be checked on each node individually. Disable SAML SSO authentication at the Jira/Confluence application level via Administration > User Management > User Directories, demote the Microsoft

SAML directory to inactive, and force local-account fallback. Document the plugin version string from the 'App Details' screen before any change as forensic baseline. For Azure AD / Entra ID, use PowerShell: Get-AzureADServicePrincipal -Filter "DisplayName eq 'Jira'" to identify the enterprise application registration and conditionally block sign-ins via Set-AzureADServicePrincipal -AccountEnabled $false as an emergency brake without removing the integration permanently.

Evidence: Before disabling the plugin, capture: (1) Atlassian application logs at /log/atlassian-jira.log and /logs/atlassian-confluence.log — export the full log files timestamped to the moment of containment; (2) current plugin version string and plugin descriptor from Administration > Manage apps > Microsoft SAML SSO > App Details; (3) a full export of current Jira project role membership and Confluence space permission schemes via the respective admin APIs (GET /rest/api/3/role and GET /wiki/rest/api/space/{spaceKey}/permission) to establish a pre-containment privilege baseline; (4) Azure AD / Entra ID Sign-in logs filtered to the Jira and Confluence enterprise application IDs for the prior 30 days, exported via Microsoft Entra admin center or MS Graph API (GET /auditLogs/signIns?$filter=appId eq '') before any session invalidation destroys evidence.

Step 2: Detection — Query Jira and Confluence access logs for anomalous privilege changes, unexpected role assignments, or administrative actions performed by non-admin accounts authenticated via SAML SSO. Review Azure AD / Entra ID sign-in logs for SAML token issuance anomalies, unexpected assertion targets, or authentication events outside normal user behavior baselines. MITRE T1078 and T1550.001 suggest looking for reuse of authentication tokens across sessions or accounts that authenticated once and then accessed resources inconsistent with their role.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, run the following directly against Atlassian logs: (1) On Linux/macOS: grep -E '(addUserToRole|removeUserFromRole|addPermission|grantProjectPermission|makeUserAdmin)' /var/atlassian/application-data/jira/log/atlassian-jira.log | grep -i 'saml' — this surfaces privilege-change audit events tied to SAML-authenticated sessions. (2) For Confluence: grep -E '(SpacePermission|GroupMembership|addAdmin)' /var/atlassian/application-data/confluence/logs/atlassian-confluence.log. (3) Enable and export Jira's built-in audit log via Administration > System > Audit Log, filter by Category 'Users and groups' and 'Permissions', export to CSV for offline analysis. (4) In Azure AD / Entra ID, use the free Microsoft Entra audit log export: navigate to Entra ID > Monitoring > Sign-in logs, filter by Application = your Jira/Confluence app registration, export to CSV, then parse with PowerShell: Import-Csv signins.csv | Where-Object { $_.ResultType -ne '0' -or $_.RiskLevelDuringSignIn -ne 'none' } | Select-Object UserDisplayName, IPAddress, Location, AppDisplayName, AuthenticationRequirement.

Evidence: Threat-specific artifacts to collect during detection: (1) Atlassian audit log entries showing 'addUserToRole', 'grantAdminPermission', or 'updateGroupMembership' actions where the actor's authentication method attribute is 'saml' and the actor is not a recognized Jira/Confluence admin account — these indicate the privilege escalation path this CVE enables; (2) Jira/Confluence session tokens (JSESSIONID values) from web server access logs (check /log/access_log*) correlated against SAML assertion subject NameIDs to identify sessions where the asserted identity does not match the elevated account's expected identity; (3) Azure AD / Entra ID Sign-in logs for SAML token issuances to the Jira/Confluence enterprise app where the token audience (Recipient attribute in the SAML assertion) or the NameID format deviates from your baseline; (4) Confluence/Jira REST API access logs for calls to privilege-granting endpoints (/rest/api/3/role/{id}/actors, /rest/usermanagement/1/group/user/direct) from authenticated sessions that were SAML-sourced; (5) Network captures (Wireshark/tcpdump) of SAML POST bindings to the Jira/Confluence Assertion Consumer Service URL if available — malformed or replayed assertions would appear as repeated POSTs to /plugins/servlet/saml/auth.

Step 3: Eradication — Apply the Microsoft-provided plugin update as directed in the MSRC May 2026 Patch Tuesday guidance. Confirm the specific patched version number from the MSRC advisory before deploying; affected version ranges are not yet confirmed in available source data. After patching, invalidate all active SAML sessions for Jira and Confluence and require re-authentication. Revoke any suspicious tokens

identified during detection review.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST SI-2 (Flaw Remediation), NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: If the Atlassian Universal Plugin Manager (UPM) cannot reach the Atlassian Marketplace due to network restrictions, download the patched plugin .obr/.jar file directly from the Microsoft GitHub releases page for the SAML SSO plugin or the MSRC advisory redirect, verify the SHA-256 hash of the downloaded file against the value published in the MSRC advisory before installing, then upload manually via Administration > Manage apps > Upload app. To invalidate all active Jira SAML sessions without a session management tool, restart the Jira/Confluence application service (systemctl restart jira or service confluence stop && service confluence start) — this flushes the in-memory session store and forces all users to re-authenticate. For Entra ID token revocation, use PowerShell: Revoke-AzureADUserAllRefreshToken -ObjectId for each account flagged during detection, or revoke all users' refresh tokens for the Jira/Confluence enterprise app via: Get-AzureADUser -All $true | ForEach-Object { Revoke-AzureADUserAllRefreshToken -ObjectId $_.ObjectId }.

Evidence: Before executing eradication, preserve: (1) a file-system snapshot or copy of the current vulnerable plugin .jar file from the Jira/Confluence plugins directory (/plugins/installed-plugins/ or equivalent) — this is the forensic baseline proving which version was running and enables later vulnerability confirmation; (2) a full export of Jira and Confluence audit logs covering the entire exposure window (from plugin installation date to patch date) via Administration > System > Audit Log, exported to an immutable storage location before the patch alters logging behavior; (3) the list of all accounts that received privilege changes during the exposure window, exported from both the Atlassian audit log and the Entra ID audit log (GET /auditLogs/directoryAudits?$filter=category eq 'RoleManagement') before token revocation removes their active session context; (4) memory dump or process snapshot of the Jira/Confluence JVM process if available (jmap -dump:format=b,file=jira_heap.hprof) on systems where active exploitation is suspected — SAML assertion content may persist in heap memory.

Step 4: Recovery — After applying the patch, validate that SAML SSO authentication flows are functioning correctly and that no privilege assignments made during the exposure window persist. Audit current role assignments in Jira and Confluence against your authoritative identity directory. Monitor authentication and privilege-change logs for 72 hours post-remediation for residual anomalies.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: To audit role assignments without an IDG/IGA tool: (1) Export all Jira project role members via the REST API: curl -u admin:token https:///rest/api/3/role | jq '.[].id' | xargs -I{} curl -u admin:token https:///rest/api/3/role/{}/actors — compare output against your HR/AD group membership export. (2) For Confluence space permissions: curl -u admin:token https:///wiki/rest/api/space?limit=100 | jq '.[].key' | xargs -I{} curl -u admin:token "https:///wiki/rest/api/space/{}/permission" — review for SAML-authenticated accounts holding admin-equivalent permissions not present in your identity directory. (3) Set up a cron job or scheduled PowerShell task to poll the Jira audit log API (GET /rest/api/3/auditing/record?limit=1000) every 15 minutes for the 72-hour monitoring window and alert on any 'addUserToRole' or 'grantPermission' events: this approximates a SIEM alert with no tooling cost.

Evidence: During the recovery validation window, continuously collect: (1) Jira and Confluence audit log entries for any permission or group change events that occur after patching — these post-patch changes would indicate either residual attacker persistence or misconfigured recovery that reintroduced escalated privileges; (2) Entra ID Conditional Access evaluation logs for the Jira/Confluence enterprise app during the 72-hour window, filtered for sign-ins that succeed despite risk flags (RiskLevelDuringSignIn = 'medium' or 'high') which may indicate compromised credentials being reused after SAML session invalidation; (3) Jira/Confluence web access logs for any requests to administrative endpoints (/secure/admin/*, /admin/*, /wiki/admin/*) from IP addresses that appeared in suspicious SAML sessions

identified during detection — post-patch admin access from these IPs would indicate backdoor accounts or persistent access mechanisms beyond the SSO vulnerability.

Step 5: Post-Incident — Review your plugin update management process; third-party SSO plugins integrated with enterprise collaboration platforms should be included in patch prioritization workflows, not treated as set-and-forget integrations. Evaluate whether SAML assertion validation controls are logged and monitored in your SIEM. Map this event to NIST CSF PR.AC-1 (identity management) and DE.AE-2 (anomaly detection) as a control gap reference point.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST AU-2 (Event Logging), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: Implement the following no-cost process improvements: (1) Subscribe to the MSRC Security Update Guide RSS feed (https://api.msrc.microsoft.com/cvrf/v2.0/updates) and the Atlassian Security Advisory mailing list (https://www.atlassian.com/trust/security/advisories) — add these as monitored feeds in your vulnerability tracking process and assign a weekly review owner. (2) Create a Sigma rule targeting Jira/Confluence audit log data for future SAML privilege escalation detection — key fields: eventType IN ('addUserToRole','grantAdminPermission') AND authenticationMethod = 'saml' AND actorIsAdmin = false; publish to your team's shared detection repository. (3) Add the Microsoft SAML SSO plugin for Jira/Confluence to your CIS Control 2.1 software inventory as a 'high-criticality' integration requiring monthly patch review, not quarterly, given its role in identity brokering for collaboration platforms that routinely hold sensitive project data.

Evidence: For the lessons-learned record and post-incident report, preserve as a complete evidence package: (1) the full Jira and Confluence audit log exports covering the exposure window, stored in immutable archival storage per NIST AU-11 (Audit Record Retention) requirements; (2) a reconciled diff of Jira/Confluence role assignments between the pre-incident baseline (captured at containment) and the post-recovery validated state, documenting exactly which accounts received unauthorized privilege escalation via CVE-2026-41103; (3) Entra ID sign-in and audit logs for the enterprise app registrations used by Jira and Confluence, covering the full exposure and response window — these establish the SAML assertion issuance timeline needed for any regulatory breach notification analysis; (4) the vulnerable plugin .jar file preserved from eradication step, stored offline as proof of the affected version for regulatory or legal documentation.

Detection Guidance

Focus detection on three surfaces: (1) Jira/Confluence audit logs, look for privilege escalation events, role additions, or admin-level actions performed by accounts with no prior administrative history, particularly those authenticated via SAML SSO. (2) Entra ID / Azure AD sign-in logs, filter for SAML token issuances to Atlassian service provider endpoints; flag tokens with unusual lifetimes, replayed assertion IDs, or issuances outside business hours. (3) MITRE T1550.001 (Pass the Token), monitor for authentication events where a user's session token appears to be reused from a different IP, user agent, or geographic location than the original authentication event. No confirmed IOCs or exploitation signatures are publicly available at this time; behavioral anomaly detection is the primary viable approach until technical root cause details and exploitation signatures are published.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1550.001** — Application Access Token

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

CIS-V8

- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1550.001	Application Access Token	Defense-Evasion

Sources

Source	URL	Tier
MSRC Update Guide	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-41103	T1
(consolidated)	https://api.msrc.microsoft.com/cvrf/v3.0/cvrf/2026-May	T1
(consolidated)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-40402	T1
(consolidated)	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2026-42823	T1
CVE-2026-43103	https://access.redhat.com/security/cve/cve-2026-43103	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2026-41103	T1

Generated 2026-05-12 14:09 UTC by TJS Security Command Center