Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0034

Kwetsbaarheden verholpen in Atlassian producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 22-01-2026

TLP:WHITE

Toegestane verspreiding van TLP:WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op info@ncsc.nl

Feiten

Atlassian heeft kwetsbaarheden verholpen in verschillende producten, welke gebruik maken van Oracle middleware producten zoals de Oracle Utilities Application Framework, WebLogic Server, Data Integrator en Business Intelligence Enterprise Edition.

Duiding

Deze kwetsbaarheden stellen ongeauthenticeerde aanvallers in staat om een denial of service (DoS) of om zich toegang te verschaffen tot gevoelige gegevens. Een reeks kwetsbaarheden is afkomstig van diverse Oracle-middleware software, welke in Atlassian-producten is verwerkt. Deze kwetsbaarheden zijn verholpen in de Critical Patch Update van januari 2026 van Oracle en verwerkt in de getroffen Atlassian producten.

Oplossingen

Atlassian heeft updates uitgebracht om de kwetsbaarheden te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- https://confluence.atlassian.com/security/security-bulletin-january-20-2026-1712324819.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2021-3807	7.5 HIGH
CVE-2022-25883	7.5 HIGH
CVE-2022-45693	7.5 HIGH
CVE-2024-21538	8.7 HIGH
CVE-2024-38286	7.7 HIGH
CVE-2024-45296	7.7 HIGH
CVE-2024-45801	8.3 HIGH
CVE-2025-12383	9.4 CRITICAL

CVE-2025-15284	8.7 HIGH
CVE-2025-27152	8.7 HIGH
CVE-2025-41249	7.5 HIGH
CVE-2025-48976	8.7 HIGH
CVE-2025-48989	6.9 MEDIUM
CVE-2025-49146	8.2 HIGH
CVE-2025-52434	6.3 MEDIUM
CVE-2025-52999	8.7 HIGH
CVE-2025-53689	2.1 LOW
CVE-2025-54988	9.3 CRITICAL
CVE-2025-55163	8.2 HIGH
CVE-2025-55752	7.7 HIGH
CVE-2025-64775	7.5 HIGH
CVE-2025-66516	10.0 CRITICAL
CVE-2025-9287	9.1 CRITICAL
CVE-2025-9288	9.1 CRITICAL
CVE-2026-21569	

CWE's

CWE	Beschrijving
CWE-20	Improper Input Validation
CWE-23	Relative Path Traversal
CWE-121	Stack-based Buffer Overflow
CWE-285	Improper Authorization

CWE-287	Improper Authentication
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-400	Uncontrolled Resource Consumption
CWE-404	Improper Resource Shutdown or Release
CWE-459	Incomplete Cleanup
CWE-611	Improper Restriction of XML External Entity Reference
CWE-697	Incorrect Comparison
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-787	Out-of-bounds Write
CWE-863	Incorrect Authorization
CWE-918	Server-Side Request Forgery (SSRF)
CWE-937	CWE-937
CWE-1035	CWE-1035
CWE-1321	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
CWE-1333	Inefficient Regular Expression Complexity

Getroffen producten

Atlassian
Bamboo
Bitbucket
Confluence
Crowd Server
Crucible
Fisheye

Jira

Disclaimer