Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2026-0325

Kwetsbaarheden verholpen in Atlassian producten

NCSC Security Advisory
Prioriteit: Normaal
Gepubliceerd op: 24-08-2026

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 diverse producten zoals Bamboo, Bitbucket, Confluence, Jira, Crowd en Fisheye. De kwetsbaarheden bevinden zich in diverse Third-Party producten waar eerder updates voor zijn verschenen. Atlassian heeft deze updates verwerkt in de eigen producten.

Duiding

Kwaadwillenden kunnen de kwetsbaarheden misbruiken om een Denial-of-Service te veroorzaken, willekeurige code uit te voeren middels het injecteren van scripts of malafide SQL-quieries en/of gegevens te manipuleren of toegang te krijgen tot gevoelige gegevens.

Enkele kwetsbaarheden hebben van origine een hoge CVSS score van 9 of meer en zijn door de ontwikkelaars van het kwetsbare product aanvankelijk ingeschaald als 'kritiek'. Door de wijze waarop Atlassian gebruik maakt van deze Third-party modules, is direct misbruik van deze kwetsbaarheden onwaarschijnlijker, waardoor Atlassian de risico's van misbruik voor hun producten lager inschaalt. Echter, door de grote hoeveelheid verholpen kwetsbaarheden adviseert het NCSC wel om deze updates met voorrang in te zetten, met name op systemen die toegankelijk zijn vanaf publieke infrastructuur.

Oplossingen

Atlassian heeft updates uitgebracht voor Bamboo, Bitbucket, Confluence, Jira, Crowd en Fisheye. Zie de bijgevoegde referenties voor meer informatie.

Referenties

- https://confluence.atlassian.com/security/security-bulletin-august-18-2026-1821999768.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2021-44906	9.8 CRITICAL
CVE-2022-3517	7.5 HIGH
CVE-2023-45133	9.3 CRITICAL
CVE-2025-14813	9.3 CRITICAL

CVE-2026-0603	8.3 HIGH
CVE-2026-2332	9.1 CRITICAL
CVE-2026-3505	8.7 HIGH
CVE-2026-4800	9.8 CRITICAL
CVE-2026-6321	7.5 HIGH
CVE-2026-6322	7.5 HIGH
CVE-2026-10050	8.7 HIGH
CVE-2026-12143	8.7 HIGH
CVE-2026-12151	7.5 HIGH
CVE-2026-12802	8.7 HIGH
CVE-2026-12803	8.7 HIGH
CVE-2026-12816	8.7 HIGH
CVE-2026-13149	7.7 HIGH
CVE-2026-13506	8.7 HIGH
CVE-2026-13676	7.5 HIGH
CVE-2026-14257	7.5 HIGH
CVE-2026-14682	8.7 HIGH
CVE-2026-16221	7.5 HIGH
CVE-2026-18446	7.5 HIGH
CVE-2026-21582	8.8 HIGH
CVE-2026-24734	7.5 HIGH
CVE-2026-25639	7.5 HIGH
CVE-2026-27601	8.2 HIGH

CVE-2026-27606	8.8 HIGH
CVE-2026-29786	8.2 HIGH
CVE-2026-40983	7.5 HIGH
CVE-2026-40984	7.5 HIGH
CVE-2026-41284	7.5 HIGH
CVE-2026-41842	7.5 HIGH
CVE-2026-41845	7.1 HIGH
CVE-2026-41850	7.5 HIGH
CVE-2026-41851	7.5 HIGH
CVE-2026-41907	8.1 HIGH
CVE-2026-42033	7.4 HIGH
CVE-2026-42035	7.4 HIGH
CVE-2026-42041	8.2 HIGH
CVE-2026-42198	7.5 HIGH
CVE-2026-42583	7.5 HIGH
CVE-2026-42587	7.5 HIGH
CVE-2026-43513	7.5 HIGH
CVE-2026-44249	8.1 HIGH
CVE-2026-44486	7.5 HIGH
CVE-2026-44487	8.2 HIGH
CVE-2026-44488	7.5 HIGH
CVE-2026-44490	8.2 HIGH
CVE-2026-44492	8.6 HIGH

CVE-2026-44494	8.7 HIGH
CVE-2026-44495	7.0 HIGH
CVE-2026-44496	7.5 HIGH
CVE-2026-45416	7.5 HIGH
CVE-2026-45623	7.5 HIGH
CVE-2026-46625	7.5 HIGH
CVE-2026-47838	6.8 MEDIUM
CVE-2026-48043	7.5 HIGH
CVE-2026-48779	7.5 HIGH
CVE-2026-48801	8.7 HIGH
CVE-2026-50010	7.5 HIGH
CVE-2026-53434	9.1 CRITICAL
CVE-2026-54291	8.2 HIGH
CVE-2026-54512	8.1 HIGH
CVE-2026-54513	8.1 HIGH
CVE-2026-55685	8.7 HIGH
CVE-2026-55831	7.5 HIGH
CVE-2026-55833	7.5 HIGH
CVE-2026-56745	8.7 HIGH
CVE-2026-56819	7.5 HIGH
CVE-2026-58059	8.7 HIGH
CVE-2026-58060	8.7 HIGH
CVE-2026-59639	8.7 HIGH

CVE-2026-59642	8.7 HIGH
CVE-2026-59869	7.5 HIGH
CVE-2026-59871	7.5 HIGH
CVE-2026-59873	9.2 CRITICAL
CVE-2026-59874	8.7 HIGH
CVE-2026-59887	7.5 HIGH
CVE-2026-59901	8.7 HIGH
CVE-2026-67320	8.3 HIGH
CVE-2026-69152	7.5 HIGH
CVE-2026-69192	7.7 HIGH

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
CWE-93	Improper Neutralization of CRLF Sequences ('CRLF Injection')
CWE-122	Heap-based Buffer Overflow
CWE-140	Improper Neutralization of Delimiters
CWE-347	Improper Verification of Cryptographic Signature
CWE-354	Improper Validation of Integrity Check Value
CWE-401	Missing Release of Memory after Effective Lifetime
CWE-407	Inefficient Algorithmic Complexity
CWE-409	Improper Handling of Highly Compressed Data (Data Amplification)

CWE-436	Interpretation Conflict
CWE-551	Incorrect Behavior Order: Authorization Before Parsing and Canonicalization
CWE-636	Not Failing Securely ('Failing Open')
CWE-670	Always-Incorrect Control Flow Implementation
CWE-674	Uncontrolled Recursion
CWE-757	Selection of Less-Secure Algorithm During Negotiation ('Algorithm Downgrade')
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-772	Missing Release of Resource after Effective Lifetime
CWE-787	Out-of-bounds Write
CWE-789	Memory Allocation with Excessive Size Value
CWE-823	Use of Out-of-range Pointer Offset
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')
CWE-911	Improper Update of Reference Count
CWE-915	Improperly Controlled Modification of Dynamically-Determined Object Attributes
CWE-918	Server-Side Request Forgery (SSRF)
CWE-940	Improper Verification of Source of a Communication Channel
CWE-1285	Improper Validation of Specified Index, Position, or Offset in Input
CWE-1289	Improper Validation of Unsafe Equivalence in Input
CWE-1321	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')

Getroffen producten

Atlassian
Bamboo
Bitbucket

Bitbucket Data Center
Confluence
Confluence Data Center
Crowd Data Center
Crucible
Fisheye
Jira
Jira Service Management Data Center
Jira Service Management Server
Jira Software Data Center
Jira Software Server

Disclaimer