Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Advisory NCSC-2026-0496

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in Atlassian producten

Publicatiedatum: 18-11-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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.

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 9.0 of hoger 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-november-17-2026-1874690748.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2015-0899	7.5 HIGH
CVE-2016-1181	8.1 HIGH
CVE-2016-1182	8.2 HIGH
CVE-2023-49735	7.5 HIGH
CVE-2026-2332	9.1 CRITICAL
CVE-2026-4800	9.8 CRITICAL
CVE-2026-8798	8.7 HIGH
CVE-2026-9563	7.5 HIGH
CVE-2026-12185	7.1 HIGH
CVE-2026-12803	8.7 HIGH
CVE-2026-12816	8.7 HIGH
CVE-2026-12860	8.7 HIGH
CVE-2026-13505	8.7 HIGH
CVE-2026-13506	8.7 HIGH
CVE-2026-14682	8.7 HIGH
CVE-2026-16633	8.6 HIGH
CVE-2026-18660	8.8 HIGH
CVE-2026-19203	8.3 HIGH
CVE-2026-21590	8.7 HIGH
CVE-2026-21591	7.4 HIGH
CVE-2026-21593	7.7 HIGH
CVE-2026-21594	8.7 HIGH
CVE-2026-21596	7.7 HIGH
CVE-2026-21598	8.7 HIGH
CVE-2026-21599	7.5 HIGH
CVE-2026-21600	8.9 HIGH
CVE-2026-21601	8.7 HIGH
CVE-2026-21602	7.4 HIGH

CVE	CVSS Score
CVE-2026-21603	8.4 HIGH
CVE-2026-21605	8.7 HIGH
CVE-2026-21606	8.7 HIGH
CVE-2026-21607	8.7 HIGH
CVE-2026-21609	7.1 HIGH
CVE-2026-40984	7.5 HIGH
CVE-2026-41695	7.5 HIGH
CVE-2026-41720	7.4 HIGH
CVE-2026-47759	8.7 HIGH
CVE-2026-47761	8.7 HIGH
CVE-2026-47762	8.7 HIGH
CVE-2026-47884	9.8 CRITICAL
CVE-2026-47885	7.5 HIGH
CVE-2026-47886	7.5 HIGH
CVE-2026-47889	7.5 HIGH
CVE-2026-47890	9.8 CRITICAL
CVE-2026-54399	7.5 HIGH
CVE-2026-54428	7.5 HIGH
CVE-2026-54512	8.1 HIGH
CVE-2026-54513	8.1 HIGH
CVE-2026-55153	7.5 HIGH
CVE-2026-55957	7.3 HIGH
CVE-2026-58059	8.7 HIGH
CVE-2026-58060	8.7 HIGH
CVE-2026-58061	8.7 HIGH
CVE-2026-59083	9.1 CRITICAL
CVE-2026-59084	9.1 CRITICAL
CVE-2026-59282	7.5 HIGH
CVE-2026-59283	9.8 CRITICAL
CVE-2026-59313	9.8 CRITICAL
CVE-2026-59639	8.7 HIGH

CVE	CVSS Score
CVE-2026-59642	8.7 HIGH
CVE-2026-59651	7.1 HIGH
CVE-2026-59901	8.7 HIGH
CVE-2026-62243	8.7 HIGH
CVE-2026-65183	8.1 HIGH
CVE-2026-65905	9.8 CRITICAL
CVE-2026-65927	8.2 HIGH
CVE-2026-66422	8.1 HIGH
CVE-2026-67213	8.2 HIGH
CVE-2026-67214	8.2 HIGH
CVE-2026-68494	8.7 HIGH
CVE-2026-68495	7.5 HIGH
CVE-2026-68496	7.5 HIGH
CVE-2026-68497	7.5 HIGH
CVE-2026-68498	7.5 HIGH
CVE-2026-68569	8.2 HIGH
CVE-2026-71290	9.1 CRITICAL
CVE-2026-71883	8.2 HIGH
CVE-2026-71884	8.2 HIGH
CVE-2026-71888	8.7 HIGH
CVE-2026-71889	8.7 HIGH
CVE-2026-73086	7.4 HIGH
CVE-2026-73646	7.5 HIGH
CVE-2026-75595	9.1 CRITICAL
CVE-2026-75596	8.7 HIGH
CVE-2026-75973	7.3 HIGH
CVE-2026-76183	9.8 CRITICAL
CVE-2026-76184	8.2 HIGH
CVE-2026-77711	8.2 HIGH
CVE-2026-77762	8.1 HIGH
CVE-2026-77791	7.5 HIGH

CVE	CVSS Score
CVE-2026-78383	7.5 HIGH
CVE-2026-78437	7.3 HIGH
CVE-2026-79677	7.5 HIGH
CVE-2026-80353	7.3 HIGH
CVE-2026-84292	7.5 HIGH
CVE-2026-84394	7.5 HIGH
CVE-2026-86248	9.8 CRITICAL
CVE-2026-86350	9.1 CRITICAL
CVE-2026-87018	7.5 HIGH
CVE-2026-87022	7.5 HIGH
CVE-2026-88041	8.2 HIGH
CVE-2026-89407	7.5 HIGH
CVE-2026-89425	7.5 HIGH
CVE-2026-90559	8.7 HIGH
CVE-2026-91403	9.1 CRITICAL
CVE-2026-91776	7.5 HIGH
CVE-2026-91777	7.5 HIGH
CVE-2026-93446	8.7 HIGH
CVE-2026-93452	8.7 HIGH
CVE-2026-93488	7.5 HIGH
CVE-2026-93491	7.5 HIGH
CVE-2026-93558	7.5 HIGH
CVE-2026-93565	7.5 HIGH
CVE-2026-93567	7.5 HIGH
CVE-2026-93568	7.5 HIGH
CVE-2026-93569	8.2 HIGH
CVE-2026-93687	8.7 HIGH
CVE-2026-93752	8.7 HIGH
CVE-2026-93753	8.7 HIGH
CVE-2026-94114	8.2 HIGH
CVE-2026-101296	9.1 CRITICAL

CVE	CVSS Score
CVE-2026-101356	9.1 CRITICAL
CVE-2026-102276	7.5 HIGH
CVE-2026-102278	7.5 HIGH
CVE-2026-103119	9.1 CRITICAL
CVE-2026-104711	9.8 CRITICAL
CVE-2026-104714	8.8 HIGH
CVE-2026-104847	8.5 HIGH
CVE-2026-104852	8.2 HIGH
CVE-2026-108106	8.7 HIGH
CVE-2026-109383	9.1 CRITICAL
CVE-2026-109869	7.5 HIGH
CVE-2026-110879	9.8 CRITICAL
CVE-2026-111755	8.2 HIGH
CVE-2026-111756	8.2 HIGH
CVE-2026-114111	8.9 HIGH
CVE-2026-114112	8.9 HIGH
CVE-2026-114113	8.4 HIGH
CVE-2026-116539	8.2 HIGH
CVE-2026-116541	8.2 HIGH
CVE-2026-118664	8.2 HIGH

CWE's

CWE	Beschrijving
CWE-22	Improper Limitation of a Pathname to a Restricted Directory
CWE-77	Improper Neutralization of Special Elements used in a Command
CWE-78	Improper Neutralization of Special Elements used in an OS Command
CWE-79	Improper Neutralization of Input During Web Page Generation

CWE	Beschrijving
CWE-93	Improper Neutralization of CRLF Sequences
CWE-94	Improper Control of Generation of Code
CWE-116	Improper Encoding or Escaping of Output
CWE-120	Buffer Copy without Checking Size of Input
CWE-122	Heap-based Buffer Overflow
CWE-125	Out-of-bounds Read
CWE-127	Buffer Under-read
CWE-130	Improper Handling of Length Parameter Inconsistency
CWE-140	Improper Neutralization of Delimiters
CWE-172	Improper Encoding or Decoding of Data
CWE-177	Improper Handling of URL Encoding (Hex Encoding)
CWE-178	Improper Handling of Case Sensitivity
CWE-180	Incorrect Behavior Order: Validate Before Canonicalize
CWE-184	Incomplete List of Disallowed Inputs
CWE-185	Incorrect Regular Expression
CWE-190	Integer Overflow or Wraparound
CWE-193	Off-by-one Error
CWE-201	Insertion of Sensitive Information Into Sent Data
CWE-212	Improper Removal of Sensitive Information Before Storage or Transfer
CWE-248	Uncaught Exception
CWE-289	Authentication Bypass by Alternate Name
CWE-294	Authentication Bypass by Capture-replay
CWE-295	Improper Certificate Validation
CWE-297	Improper Validation of Certificate with Host Mismatch
CWE-303	Incorrect Implementation of Authentication Algorithm
CWE-304	Missing Critical Step in Authentication
CWE-305	Authentication Bypass by Primary Weakness
CWE-323	Reusing a Nonce, Key Pair in Encryption
CWE-326	Inadequate Encryption Strength
CWE-327	Use of a Broken or Risky Cryptographic Algorithm
CWE-347	Improper Verification of Cryptographic Signature
CWE-349	Acceptance of Extraneous Untrusted Data With Trusted Data

CWE	Beschrijving
CWE-354	Improper Validation of Integrity Check Value
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-386	Symbolic Name not Mapping to Correct Object
CWE-404	Improper Resource Shutdown or Release
CWE-407	Inefficient Algorithmic Complexity
CWE-416	Use After Free
CWE-436	Interpretation Conflict
CWE-441	Unintended Proxy or Intermediary
CWE-444	Inconsistent Interpretation of HTTP Requests
CWE-459	Incomplete Cleanup
CWE-467	Use of sizeof() on a Pointer Type
CWE-470	Use of Externally-Controlled Input to Select Classes or Code
CWE-475	Undefined Behavior for Input to API
CWE-488	Exposure of Data Element to Wrong Session
CWE-502	Deserialization of Untrusted Data
CWE-601	URL Redirection to Untrusted Site
CWE-606	Unchecked Input for Loop Condition
CWE-617	Reachable Assertion
CWE-674	Uncontrolled Recursion
CWE-754	Improper Check for Unusual or Exceptional Conditions
CWE-757	Selection of Less-Secure Algorithm During Negotiation
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-772	Missing Release of Resource after Effective Lifetime
CWE-776	Improper Restriction of Recursive Entity References in DTDs
CWE-787	Out-of-bounds Write
CWE-789	Memory Allocation with Excessive Size Value
CWE-807	Reliance on Untrusted Inputs in a Security Decision
CWE-823	Use of Out-of-range Pointer Offset
CWE-829	Inclusion of Functionality from Untrusted Control Sphere
CWE-835	Loop with Unreachable Exit Condition
CWE-839	Numeric Range Comparison Without Minimum Check

CWE	Beschrijving
CWE-862	Missing Authorization
CWE-913	Improper Control of Dynamically-Managed Code Resources
CWE-915	Improperly Controlled Modification of Dynamically-Determined Object Attributes
CWE-917	Improper Neutralization of Special Elements used in an Expression Language Statement
CWE-918	Server-Side Request Forgery
CWE-1025	Comparison Using Wrong Factors
CWE-1050	Excessive Platform Resource Consumption within a Loop
CWE-1104	Use of Unmaintained Third Party Components
CWE-1188	Initialization of a Resource with an Insecure Default
CWE-1240	Use of a Cryptographic Primitive with a Risky Implementation
CWE-1241	Use of Predictable Algorithm in Random Number Generator
CWE-1275	Sensitive Cookie with Improper SameSite Attribute
CWE-1284	Improper Validation of Specified Quantity in Input
CWE-1289	Improper Validation of Unsafe Equivalence in Input
CWE-1321	Improperly Controlled Modification of Object Prototype Attributes
CWE-1322	Use of Blocking Code in Single-threaded, Non-blocking Context
CWE-1333	Inefficient Regular Expression Complexity
CWE-1336	Improper Neutralization of Special Elements Used in a Template Engine
CWE-1395	Dependency on Vulnerable Third-Party Component

Getroffen producten

Atlassian
Bamboo
Bamboo Data Center
Bitbucket
Confluence

Atlassian
Crowd Data Center
Crucible
Fisheye
Jira
Jira Core Data Center
Jira Service Management Data Center
Jira Software Data Center

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions:
NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.