Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

NCSC-2024-0466

Kwetsbaarheden verholpen in Atlassian producten

NCSC Advisory
Prioriteit: Normaal
Gepubliceerd op: 06-12-2024

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 als Jira, Bamboo en Confluence.

Duiding

De kwetsbaarheden bevinden zich in verschillende third party componenten van ontwikkelaars zoals Oracle, RedHat en het Apache consortium. Deze kwetsbaarheden kunnen leiden tot geheugenuitputting en Denial-of-Service (DoS) door onjuiste invoerbeperkingen. Aanvallers kunnen deze kwetsbaarheden misbruiken door speciaal vervaardigde verzoeken te sturen, wat kan resulteren in systeeminstabiliteit en crashes. Voor de kwetsbaarheden zijn door de diverse ontwikkelaars updates uitgebracht om ze te verhelpen. Atlassian heeft de updates verwerkt in de eigen 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-november-19-2024-1456179091.html

Kwetsbaarheden

CVE	CVSS Score
CVE-2022-38900	7.5 HIGH
CVE-2023-46234	7.5 HIGH
CVE-2023-52428	7.5 HIGH
CVE-2024-4068	
CVE-2024-21697	8.8 HIGH
CVE-2024-24549	7.5 HIGH
CVE-2024-30172	7.5 HIGH
CVE-2024-34750	7.5 HIGH

CVE-2024-38286	
CVE-2024-38816	8.1 HIGH
CVE-2024-45801	7.3 HIGH
CVE-2024-47561	9.8 CRITICAL

CWE's

CWE	Beschrijving
CWE-755	Improper Handling of Exceptional Conditions
CWE-347	Improper Verification of Cryptographic Signature
CWE-1050	Excessive Platform Resource Consumption within a Loop
CWE-23	Relative Path Traversal
CWE-1333	Inefficient Regular Expression Complexity
CWE-1321	Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution')
CWE-400	Uncontrolled Resource Consumption
CWE-770	Allocation of Resources Without Limits or Throttling
CWE-502	Deserialization of Untrusted Data
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
CWE-835	Loop with Unreachable Exit Condition ('Infinite Loop')
CWE-20	Improper Input Validation

Getroffen producten

atlassian
atlassian_bamboo__10.0.0
atlassian_bamboo__9.2.17

atlassian_bamboo__9.6.4
atlassian_bitbucket__8.19.9
atlassian_bitbucket__8.9.19
atlassian_bitbucket__9.0.0
atlassian_confluence__7.19.26
atlassian_confluence__7.19.26__lts_
atlassian_confluence__8.5.12
atlassian_confluence__8.5.14__lts_
atlassian_confluence__8.9.4
atlassian_confluence__9.0.1
atlassian_confluence_data_center__9.0.1
atlassian_jira_software__9.12.12__lts_
atlassian_jira_software__9.4.25__lts_
atlassian_jira_software_data_center__9.17.1
atlassian_jira_software_service_management__5.12.12__lts_
atlassian_jira_software_service_management__5.4.25__lts_
atlassian_jira_software_service_management_data_center__5.17.1
bamboo
bitbucket
confluence
jira_software
sourcetree
sourcetree_for_mac
sourcetree_for_windows

Disclaimer