



Advisory NCSC-2026-0402

PRIORITEIT: NORMAAL

Kwetsbaarheid verholpen in Atlassian Data Center producten

Publicatiedatum: 06-10-2026

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

De kwetsbaarheid bevindt zich in meerdere producten binnen het Atlassian Data Center-platform, waaronder Jira Software, Jira Service Management, Confluence, Bitbucket, Bamboo, Crowd, Crucible en Fisheye.

Duiding

De kwetsbaarheid betreft een Arbitrary File Access-probleem waarmee ongeauthenticeerde aanvallers specifieke bestanden binnen de rootdirectory van de webapplicatie kunnen benaderen. Exploitatie vereist kennis van het exacte bestandspad en de bestandsnaam. Hierdoor kunnen mogelijk gevoelige bestanden worden uitgelezen. De kwetsbaarheid vormt daarmee een risico voor de vertrouwelijkheid van gegevens en configuratie-informatie die door de getroffen applicaties worden beheerd.

Oplossingen

Atlassian heeft patches uitgebracht in aangewezen productversies om de kwetsbaarheid te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://confluence.atlassian.com/spaces/SECURITY/pages/1870495748/CVE-2026-21589+-+Arbitrary+File+Access+Vulnerability+impacts+Multiple+Products>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-21589	9.3 CRITICAL

CWE's

CWE	Beschrijving
CWE-552	Files or Directories Accessible to External Parties

Getroffen producten

Atlassian
Bamboo
Bitbucket
Confluence
Crowd Server
Crucible
Fisheye
Jira

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 or 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.