



NCSC-2024-0231

Kwetsbaarheden verholpen in Atlassian producten

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 22-05-2024

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, zoals Jira, Confluence en Bitbucket.

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om aanvallen uit te voeren die kunnen leiden tot de volgende categorieën schade:

- Cross-Site Request Forgery (XSRF)
- Denial-of-Service (DoS)
- Omzeilen van authenticatie
- (Remote) code execution (Administrator/Root rechten)
- (Remote) code execution (Gebruikersrechten)
- SQL Injection
- Toegang tot systeemgegevens

Oplossingen

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

<https://confluence.atlassian.com/security/security-bulletin-may-21-2024-1387867145.html>

Referenties

➤ <https://confluence.atlassian.com/pages/viewpage.action?pageId=1387867145>

Kwetsbaarheden

CVE	CVSS Score
➤ CVE-2017-7656	
➤ CVE-2017-9735	
➤ CVE-2020-10672	
➤ CVE-2020-10673	
➤ CVE-2020-10968	

> CVE-2020-10969

> CVE-2020-11111

> CVE-2020-11112

> CVE-2020-11113

> CVE-2020-24616

> CVE-2020-35728

> CVE-2020-36179

> CVE-2020-36180

> CVE-2020-36181

> CVE-2020-36182

> CVE-2020-36184

> CVE-2020-36188

> CVE-2021-28165

> CVE-2022-25647

> CVE-2022-41966

> CVE-2022-42003

> CVE-2023-4759

> CVE-2023-34396

> CVE-2023-41835

> CVE-2023-45859

> CVE-2024-1597

> CVE-2024-21634

> CVE-2024-21683

[> CVE-2024-22257](#)[> CVE-2024-22262](#)[> CVE-2024-23672](#)[> CVE-2024-24549](#)

CWE's

CWE	Beschrijving
> CVE-284	Improper Access Control
> CVE-20	Improper Input Validation
> CVE-281	Improper Preservation of Permissions
> CVE-400	Uncontrolled Resource Consumption
> CVE-404	Improper Resource Shutdown or Release
> CVE-444	Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
> CVE-459	Incomplete Cleanup
> CVE-502	Deserialization of Untrusted Data
> CVE-601	URL Redirection to Untrusted Site ('Open Redirect')
> CVE-770	Allocation of Resources Without Limits or Throttling
> CVE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')
> CVE-913	Improper Control of Dynamically-Managed Code Resources
> CVE-96	Improper Neutralization of Directives in Statically Saved Code ('Static Code Injection')

Getroffen producten

atlassian
bamboo
bitbucket
confluence
crowd
jira_service_management
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 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.