



NCSC-2024-0373

Kwetsbaarheden verholpen in GitLab Enterprise Edition en Community Edition

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 13-09-2024

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

GitLab heeft kwetsbaarheden verholpen in Enterprise Edition (EE) en Community Edition (CE).

Duiding

Een kwaadwillende kan de kwetsbaarheden misbruiken om een Denial-of-Service te veroorzaken, of om zich verhoogde rechten toe te kennen en acties uit te voeren in de context van een andere gebruiker, waaronder ook mogelijk gebruikers met administrator-rechten.

Oplossingen

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

Referenties

➤ <https://about.gitlab.com/releases/2024/09/11/patch-release-gitlab-17-3-2-released/>

Kwetsbaarheden

| CVE | CVSS Score |
|---------------------------------|--------------|
| ➤ CVE-2024-4472 | 4.0 MEDIUM |
| ➤ CVE-2024-6678 | 9.9 CRITICAL |
| ➤ CVE-2024-8631 | 5.5 MEDIUM |
| ➤ CVE-2024-2743 | 5.3 MEDIUM |
| ➤ CVE-2024-4660 | 6.5 MEDIUM |
| ➤ CVE-2024-5435 | 4.5 MEDIUM |
| ➤ CVE-2024-6389 | 4.3 MEDIUM |
| ➤ CVE-2024-6685 | |
| ➤ CVE-2024-8640 | 8.5 HIGH |

| | |
|-----------------|------------|
| > CVE-2024-8635 | 7.7 HIGH |
| > CVE-2024-8641 | 6.7 MEDIUM |
| > CVE-2024-4283 | |
| > CVE-2024-4612 | 6.4 MEDIUM |
| > CVE-2024-8311 | 6.5 MEDIUM |
| > CVE-2024-6446 | 3.5 LOW |
| > CVE-2024-8124 | 7.5 HIGH |

CWE's

| CWE | Beschrijving |
|------------|---|
| > CVE-267 | Privilege Defined With Unsafe Actions |
| > CVE-840 | CWE-840 |
| > CVE-424 | Improper Protection of Alternate Path |
| > CVE-497 | Exposure of Sensitive System Information to an Unauthorized Control Sphere |
| > CVE-270 | Privilege Context Switching Error |
| > CVE-601 | URL Redirection to Untrusted Site ('Open Redirect') |
| > CVE-77 | Improper Neutralization of Special Elements used in a Command ('Command Injection') |
| > CVE-532 | Insertion of Sensitive Information into Log File |
| > CVE-290 | Authentication Bypass by Spoofing |
| > CVE-862 | Missing Authorization |
| > CVE-1333 | Inefficient Regular Expression Complexity |
| > CVE-918 | Server-Side Request Forgery (SSRF) |
| > CVE-863 | Incorrect Authorization |
| > CVE-209 | Generation of Error Message Containing Sensitive Information |

Getroffen producten

| |
|----------------------------|
| gitlab |
| gitlab |
| open_source |
| open_source_gitlab__17.1.7 |
| open_source_gitlab__17.2.5 |
| open_source_gitlab__17.3.2 |

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.