



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Proof-of-Concept für kritische Schwachstelle in GitLab veröffentlicht

CSW-Nr. 2024-205245-1032, Version 1.0, 15.01.2024

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Am 11. Januar veröffentlichte GitLab ein Security Advisory [GITL24] zu kritischen Schwachstellen in GitLab Community Edition (CE) und Enterprise Edition (EE). Besonders kritisch ist die Sicherheitslücke CVE-2023-7028, die es Angreifenden erlaubt, ohne Authentifizierung Konten zu übernehmen und die daher eine CVSS-Bewertung von 10.0 ("kritisch") erhielt. Angreifende können mit nicht verifizierten Email-Adressen Passwörter zurücksetzen und somit Zugang zu Benutzerkonten erhalten, sofern keine 2-Faktor Authentifizierung aktiviert ist.

Mittlerweile wurden Proof-of-Concepts veröffentlicht [POC24], die ein sehr einfaches Ausnutzen der Schwachstelle ermöglichen. Von bereits stattfindenden Angriffen kann daher ausgegangen werden.

Betroffen sind die selbst-gehosteten GitLab Versionen:

- 16.1 - 16.1.5
- 16.2 - 16.2.8
- 16.3 - 16.3.6
- 16.4 - 16.4.4
- 16.5 - 16.5.5
- 16.6 - 16.6.3
- 16.7 - 16.7.1

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.

2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.

3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.

4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Patches wurden für die Versionen 16.1 bis 16.7 veröffentlicht, die ebenfalls weitere schwerwiegende Schwachstellen beheben [GITL24].

Bewertung

Die hohe Verbreitung und die gegebenenfalls sensitiven Informationen, die sich in Repositories befinden können, machen GitLab zu einem interessanten Ziel für Angreifende. Vor allem die einfache Ausnutzbarkeit über HTTP-Anfragen ermöglicht es, auch technisch nicht besonders versierten Angreifenden Konten zu übernehmen und Informationen zu sammeln. Wie schwerwiegend eine Kontoübernahme ist, hängt von den jeweiligen Zugriffsrechten sowie den auf GitLab abgelegten Informationen ab. Sollte GitLab als Identitätsprovider für Anmeldungen an weiteren Diensten genutzt werden, so können Angreifende mit den übernommenen Benutzerkonten auch auf diese zugreifen.

Maßnahmen

IT-Sicherheitsverantwortliche sollten schnellstmöglich die bereitstehenden Patches einspielen sowie **auf eine bereits stattgefundene Kontoübernahme prüfen**. Das BSI empfiehlt grundsätzlich, die 2-Faktor Authentifizierung für schützenswerte Konten zu aktivieren [BSI].

Patches

Folgende behebende Versionen stehen zur Verfügung:

- 16.1.6
- 16.2.9
- 16.3.7
- 16.4.5
- 16.5.6
- 16.6.4
- 16.7.2

Es sollte auf eine der genannten oder höheren Versionen aktualisiert werden [GITL24]. Sollte es nicht möglich sein, eine Aktualisierung vorzunehmen, so kann das Erzwingen von 2-Faktor Authentifizierung (2FA) als vorübergehende Lösung die Kontoübernahme durch die Schwachstelle verhindern, jedoch kann es trotzdem noch möglich sein, dass Angreifende Passwörter zurücksetzen können. Generell sollte für wichtige Konten mit hohen Privilegien 2FA aktiviert sein.

Indikatoren

Aufgrund der einfachen Ausnutzbarkeit [POC24] sollten die von GitLab bereitgestellten Indikatoren zur Prüfung auf Kompromittierung genutzt werden, um von Angreifenden übernommene Konten zu identifizieren [GITL24].

- Überprüfen Sie `gitlab-rails/production_json.log` auf die Existenz von HTTP Anfragen mit dem Pfad `"/users/password"` und dem Parameter `params.value.email` bestehend aus einem JSON-Array mit mehreren Email-Adressen.
- Überprüfen Sie `gitlab-rails/audit_json.log` auf Einträge mit `meta.caller_id` von `PasswordsController#create` und `target_details` bestehend aus einem JSON-Array mit mehreren Email-Adressen.

Links

[GITL24] GitLab Security Advisory

<https://about.gitlab.com/releases/2024/01/11/critical-security-release-gitlab-16-7-2-released/>

[WID24] WID Kurzmeldung

<https://wid.cert-bund.de/portal/wid/securityadvisory?name=WID-SEC-2024-0077>

[POC24] PoC von Vozec zu CVE-2023-7028

<https://github.com/Vozec/CVE-2023-7028>

[BSI] Technische Betrachtung 2FA

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cyber-Sicherheitsempfehlungen/Accountschutz/Zwei-Faktor-Authentisierung/Bewertung-2FA-Verfahren/bewertung-2fa-verfahren_node.html

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs), welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

Das vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.

2) Welche Einstufungen existieren?

- **TLP:CLEAR: Unbegrenzte Weitergabe**

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

- **TLP:GREEN: Organisationsübergreifende Weitergabe**

Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.

- **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**

Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe

Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

- **TLP:RED: Persönlich, nur für benannte Empfänger**

Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-ingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.