


←



Bitbucket Data Center 9.3 (Latest)

Documentation

› Get started with Bitbucket Data Center

› Use Bitbucket Data Center

› Administer Bitbucket Data Center

› Integrated CI/CD

› Install or upgrade Bitbucket

› Bitbucket Data Center

▼ Release notes

Upgrade matrix

Bitbucket Mesh compatibility matrix

› Bitbucket Data Center 9 release notes

› Bitbucket Data Center and Server 8 release notes

› Bitbucket Server 7 release notes

› Bitbucket Server 6 release notes

› Bitbucket Server 5 release notes

› Bitbucket Server 4 release notes

› Older releases

▼ Bitbucket Server security advisories

Stash security advisory 2012-09-04

Stash security advisory 2014-02-26

Bitbucket Server security advisory 2016-09-21

Bitbucket Server security advisory 2017-01-24

Bitbucket Server security advisory 2018-03-21

Bitbucket Data

Bitbucket Server and Data Center Advisory 2022-08-24

Bitbucket Server and Data Center - Command injection vulnerability - CVE-2022-36804

Summary	CVE-2022-36804 - command injection vulnerability
Advisory Release Date	24 Aug 2022 10 AM PDT (Pacific Time, -7 hours)
Product	<ul style="list-style-type: none">Bitbucket ServerBitbucket Data Center
CVE ID(s)	CVE-2022-36804

Summary of Vulnerability

This advisory discloses a critical severity security vulnerability which was introduced in version 7.0.0 of Bitbucket Server and Data Center. All versions released after 6.10.17 including 7.0.0 and newer are affected, this means that all instances that are running any versions between 7.0.0 and 8.3.0 inclusive are affected by this vulnerability.

There is a command injection vulnerability in multiple API endpoints of Bitbucket Server and Data Center. An attacker with access to a public repository or with **read** permissions to a private Bitbucket repository can execute arbitrary code by sending a malicious HTTP request.

This issue can be tracked here:
[BSERV-13438](#) - Critical severity command injection vulnerability - CVE-2022-36804 **PUBLISHED**

Atlassian Cloud sites are not affected.

If you access Bitbucket via a [bitbucket.org](#) domain, it is hosted by Atlassian and you are not affected by the vulnerability.

Severity

Atlassian rates the severity level of this vulnerability as **critical**, according to the scale published in [our Atlassian severity levels](#). The scale allows us to rank the severity as critical, high, moderate or low.

This is our assessment and you should evaluate its applicability to your own IT environment.

Affected Versions

All versions of Bitbucket Server and Datacenter released after 6.10.17 including 7.0.0 and newer are affected, this means that all instances that are running any versions between 7.0.0 and 8.3.0 inclusive are affected by this vulnerability.

Fixed Versions

Ce site utilise des cookies pour améliorer votre expérience de navigation, effectuer des analyses et des recherches, et cibler la publicité. Pour modifier vos préférences, cliquez sur [Gérer les préférences](#). Sinon, cliquez sur [Accepter tous les cookies](#) pour indiquer que vous consentez à leur utilisation sur votre appareil. Cliquez sur [Rejeter tous les cookies](#) signifie que vous n'acceptez pas que nous utilisions des cookies qui ne sont pas strictement nécessaires sur votre appareil. [Avis relatif aux cookies et au suivi d'Atlassian](#)

[Gérer les préférences](#)

Rejeter tous les cookies

Accepter tous les cookies



2020-01-15

Multiple Products
Security Advisory -



Bitbucket Data Center
9.3 (Latest)
Documentation

- › Get started with Bitbucket Data Center
- › Use Bitbucket Data Center
- › Administer Bitbucket Data Center
- › Integrated CI/CD
- › Install or upgrade Bitbucket
- › Bitbucket Data Center

▼ Release notes

- Upgrade matrix
- Bitbucket Mesh compatibility matrix
- › Bitbucket Data Center 9 release notes
- › Bitbucket Data Center and Server 8 release notes
- › Bitbucket Server 7 release notes
- › Bitbucket Server 6 release notes
- › Bitbucket Server 5 release notes
- › Bitbucket Server 4 release notes
- › Older releases

▼ Bitbucket Server security advisories

- Stash security advisory 2012-09-04
- Stash security advisory 2014-02-26
- Bitbucket Server security advisory 2016-09-21
- Bitbucket Server security advisory 2017-01-24
- Bitbucket Server security advisory 2018-03-21
- Bitbucket Data

Bitbucket Server and Data Center 8.0	8.0.3 or newer
Bitbucket Server and Data Center 8.1	8.1.3 or newer
Bitbucket Server and Data Center 8.2	8.2.2 or newer
Bitbucket Server and Data Center 8.3	8.3.1 or newer

What You Need to Do

Atlassian recommends that you upgrade your instance to one of the versions listed in the “Fixed Versions” section of this same page. For a full description of the latest version of Bitbucket Server and Data Center, see the [release notes](#). You can download the latest version of Bitbucket from the [download center](#). For Frequently Asked Questions (FAQ) [click here](#).

Bitbucket Mesh

If you have configured Bitbucket Mesh nodes, these will need to be updated with to the corresponding version of Mesh that includes the fix. To find the version of Mesh compatible with Bitbucket Data Center version, please check the [compatibility matrix](#). You can download the corresponding version from the [download center](#).

If you are unsure if your Bitbucket instance has Bitbucket Mesh configured, as a user with system administration privileges navigate to **Administration > Bitbucket Mesh**, this page will list Mesh nodes each of which will need to be upgraded. **If the list is empty, your instance does not have Mesh configured and this extra step is not required.**

Mitigation

To remediate this vulnerability, update each affected product installation to a fixed version listed above.

If you’re unable to upgrade Bitbucket, [a temporary mitigation step is to turn off public repositories globally](#) by setting ***feature.public.access=false*** as this will change this attack vector from an unauthorized attack to an authorized attack. This can not be considered a complete mitigation as an attacker with a user account could still succeed.

Acknowledgments

This vulnerability was discovered by [@TheGrandPew](#) and reported via our Bug Bounty program.

Support

If you did not receive an email for this advisory and you wish to receive such emails in the future go to <https://my.atlassian.com/email> and subscribe to Alerts emails.

If you have questions or concerns regarding this advisory, please raise a support request at <https://support.atlassian.com/>.

References

Security Bug fix Policy	As per our new policy critical security bug fixes will be back ported in accordance with https://www.atlassian.com/trust/security/bug-fix-policy . We will release new maintenance releases for the versions covered by the policy instead of binary patches. Binary patches are no longer released.
Severity Levels for	Atlassian security advisories include a severity level and a CVE identifier. This severity level is based on our self-calculated CVSS score for each specific

Ce site utilise des cookies pour améliorer votre expérience de navigation, effectuer des analyses et des recherches, et cibler la publicité. Pour modifier vos préférences, cliquez sur Gérer les préférences. Sinon, cliquez sur Accepter tous les cookies pour indiquer que vous consentez à leur utilisation sur votre appareil. Cliquez sur Rejeter tous les cookies signifie que vous n'acceptez pas que nous utilisions des cookies qui ne sont pas strictement nécessaires sur votre appareil. [Avis relatif aux cookies et au suivi d'Atlassian](#)

2020-01-15

2020-01-15

Multiple Products
Security Advisory -



Bitbucket Data Center
9.3 (Latest)
Documentation

- › Get started with Bitbucket Data Center
- › Use Bitbucket Data Center
- › Administer Bitbucket Data Center
- › Integrated CI/CD
- › Install or upgrade Bitbucket
- › Bitbucket Data Center

▼ Release notes

- Upgrade matrix
- Bitbucket Mesh compatibility matrix
- › Bitbucket Data Center 9 release notes
- › Bitbucket Data Center and Server 8 release notes
- › Bitbucket Server 7 release notes
- › Bitbucket Server 6 release notes
- › Bitbucket Server 5 release notes
- › Bitbucket Server 4 release notes
- › Older releases

▼ Bitbucket Server security advisories

- Stash security advisory 2012-09-04
- Stash security advisory 2014-02-26
- Bitbucket Server security advisory 2016-09-21
- Bitbucket Server security advisory 2017-01-24
- Bitbucket Server security advisory 2018-03-21
- Bitbucket Data

Was this helpful?

Yes

No

[Provide feedback about this article](#)

Related content

- Use Bitbucket in the enterprise
- High availability for Bitbucket
- Running Bitbucket Data Center on a single node
- Upgrade Bitbucket from an archive file
- Install Bitbucket Data Center from an archive file
- Link Bitbucket with Jira
- Bitbucket Data Center and Server feature comparison
- Clustering with Bitbucket
- Migrating Bitbucket Data Center to another server
- Install Bitbucket Data Center on Linux from an archive file

Powered by [Confluence](#) and [Scroll Viewport](#).

[Your Privacy Choices](#)

[Privacy Policy](#)

[Terms of Use](#)

[Security](#)

© 2024 Atlassian

Ce site utilise des cookies pour améliorer votre expérience de navigation, effectuer des analyses et des recherches, et cibler la publicité. Pour modifier vos préférences, cliquez sur [Gérer les préférences](#). Sinon, cliquez sur [Accepter tous les cookies](#) pour indiquer que vous consentez à leur utilisation sur votre appareil. Cliquez sur [Rejeter tous les cookies](#) signifie que vous n'acceptez pas que nous utilisions des cookies qui ne sont pas strictement nécessaires sur votre appareil. [Avis relatif aux cookies et au suivi d'Atlassian](#)

2020-01-15