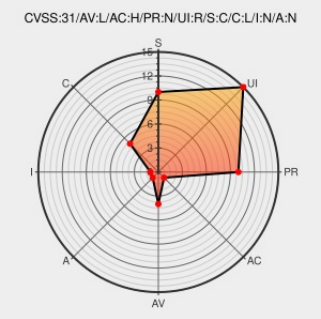
CVE-2021-32825

Published on: 08/16/2021 12:00:00 AM UTC

Last Modified on: 07/02/2022 06:22:00 PM UTC

CVE-2021-32825 - advisory for GHSL-2020-258

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Bblfshd from Bblfshd Project contain the following vulnerability:

bblfshd is an open source self-hosted server for source code parsing. In bblfshd before commit 4265465b9b6fb5663c30ee43806126012066aad4 there is a "zipslip" vulnerability. The unsafe handling of symbolic links in an unpacking routine may enable attackers to read and/or write to arbitrary locations outside the designated target folder. This issue may lead to arbitrary file write (with same permissions as the program running the unpack operation) if the attacker can control the archive file. Additionally, if the attacker has read access to the unpacked files, he may be able to read arbitrary system files the parent process has permissions to read. For more details including a PoC see the referenced GHSL-2020-258.

CVE-2021-32825 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **bblfsh** - **bblfshd** version **< 4265465b9b6fb5663c30ee43806126012066aad4**

CVSS3 Score: 9.1 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	NONE

CVSS2 Score: 5.5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
untar: add check on link · bblfsh/bblfshd@4265465 · GitHub	github.com text/html	MISC github.com/bblfsh/bblfshd/commit/4265465b9b6fb5663c30ee43806126012066aad4
Bugfix ghsl 2020 258 by david972 · Pull Request #341 · bblfsh/bblfshd · GitHub	github.com text/html	MISC github.com/bblfsh/bblfshd/pull/341
GHSL-2020-258: ZipSlip vulnerability in bblfshd - CVE-2021-32825 | GitHub Security Lab	securitylab.github.com text/html	CONFIRM securitylab.github.com/advisories/GHSL-2020-258-zipslip-bblfshd/

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bblfshd Project	Bblfshd	All	All	All	All

cpe:2.3:a:bblfshd_project:bblfshd:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@GHSecurityLab	GHSL-2020-258: ZipSlip vulnerability in bblfshd - CVE-2021-32825 github.co/3kIPy0H	2021-07-21 20:00:15
@CVEreport	CVE-2021-32825 : bblfshd is an open source self-hosted server for source code parsing. In bblfshd before commit 426… twitter.com/i/web/status/1…	2021-08-16 19:16:23

← Previous ID Next ID→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report