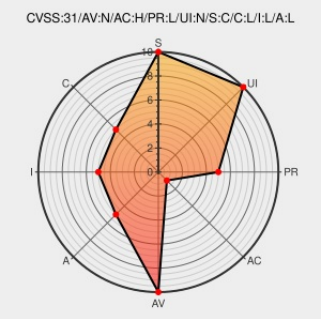
CVE-2020-11061

Published on: 07/10/2020 12:00:00 AM UTC

Last Modified on: 01/27/2023 07:11:00 PM UTC

CVE-2020-11061 - advisory for GHSA-mm45-cg35-54j4

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



Certain versions of Bareos from Bareos contain the following vulnerability:

In Bareos Director less than or equal to 16.2.10, 17.2.9, 18.2.8, and 19.2.7, a heap overflow allows a malicious client to corrupt the director's memory via oversized digest strings sent during initialization of a verify job. Disabling verify jobs mitigates the problem. This issue is also patched in Bareos versions 19.2.8, 18.2.9 and 17.2.10.

CVE-2020-11061 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Bareos GmbH & Co. KG** - **Bareos Director** version **<= 16.2.10**

Affected Vendor/Software: **Bareos GmbH & Co. KG** - **Bareos Director** version **<= 17.2.9**

Affected Vendor/Software: **Bareos GmbH & Co. KG** - **Bareos Director** version **<= 18.2.8**

Affected Vendor/Software: **Bareos GmbH & Co. KG** - **Bareos Director** version **<= 19.2.7**

CVSS3 Score: 7.4 - HIGH

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

CVSS2 Score: 6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
0001210: Security vulnerability results in heap overflow in director when doing a Verify job against a file daemon. - Bareos Bug Tracker	Vendor Advisory bugs.bareos.org text/html	MISC bugs.bareos.org/view.php?id=1210
Heap overflow in director when running a verify job against a malicious filedaemon · Advisory · bareos/bareos · GitHub	Third Party Advisory github.com text/html	CONFIRM github.com/bareos/bareos/security/advisories/GHSA-mm45-cg35-54j4
[SECURITY] [DLA 2353-1] bacula security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20200829 [SECURITY] [DLA 2353-1] bacula security update

Related QID Numbers

501177 Alpine Linux Security Update for bareos

501528 Alpine Linux Security Update for bareos

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bareos	Bareos	18.2.4	rc1	All	All
Application	Bareos	Bareos	18.2.4	rc2	All	All
Application	Bareos	Bareos	18.2.4	rc1	All	All
Application	Bareos	Bareos	18.2.4	rc2	All	All
Application	Bareos	Bareos	All	All	All	All
Application	Bareos	Bareos	All	All	All	All
Application	Bareos	Bareos	All	All	All	All
Application	Bareos	Bareos	All	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All

cpe:2.3:a:bareos:bareos:18.2.4:rc1:*:*:*:*:*:*:

cpe:2.3:a:bareos:bareos:18.2.4:rc2:*:*:*:*:*:*:

cpe:2.3:a:bareos:bareos:18.2.4:rc1:*:*:*:*:*:*:

cpe:2.3:a:bareos:bareos:18.2.4:rc2:*:*:*:*:*:*:

cpe:2.3:a:bareos:bareos:*:*:*:*:*:*:*:*:

cpe:2.3:a:bareos:bareos:*:*:*:*:*:*:*:*:

cpe:2.3:a:bareos:bareos:*:*:*:*:*:*:*:*:

cpe:2.3:a:bareos:bareos:*:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→