

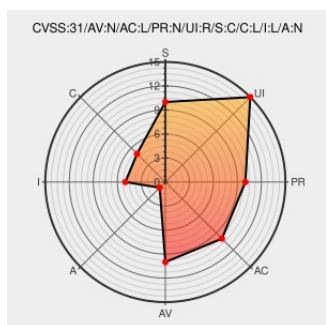


CVE-2020-8120

Published on: 02/04/2020 12:00:00 AM UTC

Last Modified on: 05/11/2023 02:00:00 PM UTC

CVE-2020-8120

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Nextcloud](#) from [Nextcloud](#) contain the following vulnerability:

A reflected Cross-Site Scripting vulnerability in Nextcloud Server 16.0.1 was discovered in the svg generation.

CVE-2020-8120 has been assigned by [h1 support@hackerone.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

CVSS3 Score: **6.1 - MEDIUM**

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

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
HackerOne	Exploit Third Party Advisory hackerone.com text/html	h1 MISC hackerone.com/reports/605915

