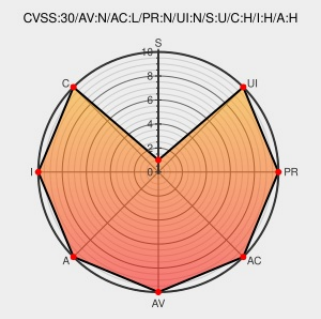
CVE-2018-9160

Published on: 03/31/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:55 PM UTC

CVE-2018-9160

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



Certain versions of Sickrage from Sickrage contain the following vulnerability:

SickRage before v2018.03.09-1 includes cleartext credentials in HTTP responses.

CVE-2018-9160 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
SickRage < v2018.03.09 - Clear-Text Credentials HTTP Response - Linux webapps Exploit	Exploit, Third Party Advisory, VDB Entry, www.exploit-db.com, Proof of Concept	EXPLOIT-DB 44545

	text/html	
Hide passwords in plain html, for when SR is not password protected (… · SiCKRAGE/SiCKRAGE@8156a74 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/SickRage/SickRage/commit/8156a74a68aea930d1e1047baba8
Page not found · GitHub · GitHub	Broken Link Third Party Advisory github.com text/html Inactive Link Not Archived	MISC github.com/SickRage/sickrage.github.io/blob/master/sickrage-news/CHANGES.md

There are currently no QIDs associated with this CVE

Exploit/POC from Github

CVE-2018-9160

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Sickrage	Sickrage	All	All	All	All

cpe:2.3:a:sickrage:sickrage:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→