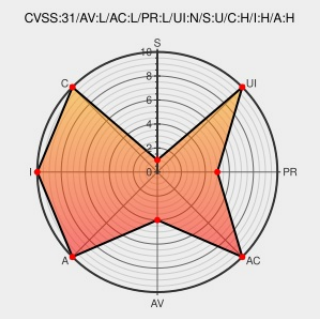
CVE-2020-27985

Published on: 11/23/2020 12:00:00 AM UTC

Last Modified on: 07/21/2021 11:39:00 AM UTC

CVE-2020-27985

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



Certain versions of Security Onion from Securityonionsolutions contain the following vulnerability:

Security Onion v2 prior to 2.3.10 has an incorrect sudo configuration, which allows the administrative user to obtain root access without using the sudo password by editing and executing /home/<user>/SecurityOnion/setup/so-setup.

CVE-2020-27985 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication
LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
CVE-2020-27985 - Security Onion - Local Privilege Escalation	Exploit, Patch, Third Party Advisory, s1gh.sh, text/html	MISC s1gh.sh/cve-2020-27985-security-onion-local-privilege-escalation/

Releases · Security-Onion-Solutions/securityonion · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/Security-Onion-Solutions/securityonion/releases
[feat] Remove so-setup permission from sudoers file after iso setup · Security-Onion-Solutions/securityonion@b146700 · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/Security-Onion-Solutions/securityonion/commit/b14670030349a2747a00ace665568ab5f51ac47b

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Securityonionsolutions	Security Onion	All	All	All	All
Application	Securityonionsolutions	Security Onion	All	All	All	All

cpe:2.3:a:securityonionsolutions:security_onion:*:*:*:*:*:*:*:*:

cpe:2.3:a:securityonionsolutions:security_onion:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→