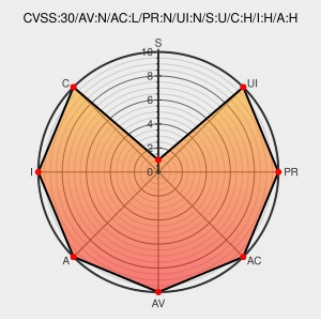
CVE-2018-1000043

Published on: 02/09/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:30 PM UTC

CVE-2018-1000043

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



Certain versions of Squert from Securityonion contain the following vulnerability:

Security Onion Solutions Squert version 1.0.1 through 1.6.7 contains a CWE-78: Improper Neutralization of Special Elements used in an OS Command (OS Command Injection) vulnerability in .inc/callback.php that can result in execution of OS Commands. This attack appear to be exploitable via Web request to .inc/callback.php with the payload in the txdata parameter, used in tx()/transcript(), or the catdata parameter, used in cat(). This vulnerability appears to have been fixed in 1.7.0.

CVE-2018-1000043 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: 10 - HIGH

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

CVE References

Description	Tags	Link
Security Onion: Security Advisory for		CONFIRM blog.securityonion.net/2018/01/security-advisory-for

Security Onion: Security Advisory for Squert	Patch Vendor Advisory blog.securityonion.net text/html	CONFIRM blog.securityonion.net/2018/01/security-advisory-for-squert.html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Securityonion	Squert	All	All	All	All

cpe:2.3:a:securityonion:squert:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→