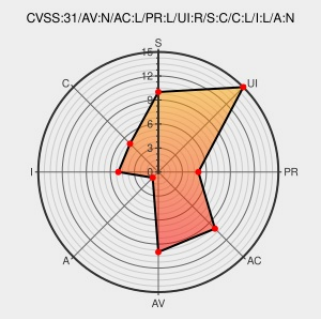
CVE-2019-19457

Published on: 12/03/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:54 PM UTC

CVE-2019-19457

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



Certain versions of Proaccess Space from Saltosystem contain the following vulnerability:

SALTO ProAccess SPACE 5.4.3.0 allows XSS.

CVE-2019-19457 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.4 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

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

CVE References

Description	Tags	Link
SALTO ProAccess SPACE 5.5 Traversal / File Write / XSS / Bypass ≈ Packet Storm	Exploit, Third Party Advisory, VDB Entry, packetstormsecurity.com, text/html	MISC packetstormsecurity.com/files/155525/SALTO-ProAccess-SPACE-5.5-Traversal-File-Write-XSS-Bypass.html

Vulnerability Lab - SEC Consult	Exploit Third Party Advisory sec-consult.com text/html	MISC sec-consult.com/en/vulnerability-lab/advisories/index.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Saltosystem	Proaccess Space	All	All	All	All

cpe:2.3:a:saltosystem:proaccess_space:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→