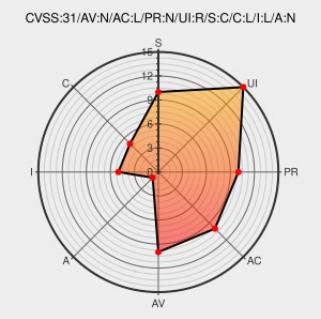
CVE-2020-13260

Published on: 09/17/2020 12:00:00 AM UTC

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

CVE-2020-13260

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



Certain versions of Secflow-1v from Rad contain the following vulnerability:

A vulnerability in the web-based management interface of RAD SecFlow-1v through 2020-05-21 could allow an authenticated attacker to upload a JavaScript file, with a stored XSS payload, that will remain stored in the system as an OVPN file in Configuration-Services-Security-OpenVPN-Config or as the static key file in Configuration-Services-Security-OpenVPN-Static Keys. This payload will execute each time a user opens an affected web page. This could be exploited in conjunction with CVE-2020-13259.

CVE-2020-13260 has been assigned by cve@mitre.org 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
RAD SecFlow-1v SF_0200_2.3.01.26 - Persistent Cross-Site Scripting	Exploit	MISC www.exploit

RAD SecFlow-1v SF_0290_2.3.01.26 - Persistent Cross-Site Scripting - Hardware webapps Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	MISC www.exploit-db.com/exploits/48807
SecFlow-1v | Ruggedized Industrial IoT Gateway with Edge Computing | RAD	Product Vendor Advisory www.rad.com text/html	MISC www.rad.com/products/secflow-1v-IIoT-Gateway#panels-ipe-paneid-143837
RAD SecFlow-1v web-based management interface - Persistent Cross-Site Scripting (Stored-XSS) - CXSecurity.com	Exploit Third Party Advisory cxsecurity.com text/html	MISC cxsecurity.com/issue/WLB-2020090063

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
Hardware	Rad	Secflow-1v	-	All	All	All
Hardware	Rad	Secflow-1v	-	All	All	All
Operating System	Rad	Secflow-1v Firmware	os-image_sf_0290_2.3.01.26	All	All	All
Operating System	Rad	Secflow-1v Firmware	os-image_sf_0290_2.3.01.26	All	All	All

cpe:2.3:h:rad:secflow-1v:-:*:*:*:*:*:*:*:

cpe:2.3:h:rad:secflow-1v:-:*:*:*:*:*:*:*:

cpe:2.3:o:rad:secflow-1v_firmware:os-image_sf_0290_2.3.01.26:*:*:*:*:*:*:*:

cpe:2.3:o:rad:secflow-1v_firmware:os-image_sf_0290_2.3.01.26:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report