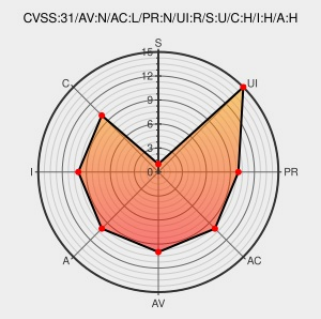
CVE-2020-13259

Published on: 09/16/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:44 PM UTC

CVE-2020-13259

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 os-image SF_0290_2.3.01.26 could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. The vulnerability is due to insufficient CSRF protections for the web UI on an affected device. An attacker could exploit this vulnerability by persuading a user of the interface to follow a malicious link. A successful exploit could allow the attacker to perform arbitrary actions with the privilege level of the affected user. This could be exploited in conjunction with CVE-2020-13260.

CVE-2020-13259 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 9.3 - HIGH

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

CVE References

Description	Tags	Link
RAD SecFlow-1v SF_0290_2.3.01.26 - Cross-Site Request Forgery (Reboot) - Hardware webapps Exploit	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 48809
RAD SecFlow-1v web-based management interface - Cross-Site Request Forgery (CSRF) - CXSecurity.com	Exploit Third Party Advisory cxsecurity.com text/html	MISC cxsecurity.com/issue/WLB-2020090064

There are currently no QIDs associated with this CVE

Exploit/POC from Github

PoC of Full Account Takeover on RAD SecFlow-1v

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→

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