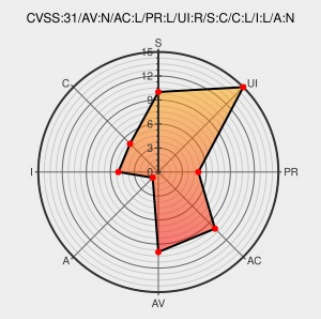
CVE-2019-18267

Published on: 12/18/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:07 PM UTC

CVE-2019-18267

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



Certain versions of S2020 from Ge contain the following vulnerability:

An issue was found in GE S2020/S2020G Fast Switch 61850, S2020/S2020G Fast Switch 61850 Versions 07A03 and prior. An attacker can inject arbitrary Javascript in a specially crafted HTTP request that may be reflected back in the HTTP response. The device is also vulnerable to a stored cross-site scripting vulnerability that may allow session hijacking, disclosure of sensitive data, cross-site request forgery (CSRF) attacks, and remote code execution.

CVE-2019-18267 has been assigned by ics-cert@hq.dhs.gov 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
GE S2020/S2020G Fast Switch 61850 | CISA	Third Party Advisory US Government Resource	MISC www.us-cert.gov/ics/advisories/icsa-19-351-01

www.us-cert.gov
text/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
Hardware	Ge	S2020	-	All	All	All
Hardware	Ge	S2020	-	All	All	All
Hardware	Ge	S2020g	-	All	All	All
Hardware	Ge	S2020g	-	All	All	All
Operating System	Ge	S2020g Firmware	All	All	All	All
Operating System	Ge	S2020 Firmware	All	All	All	All

cpe:2.3:h:ge:s2020:-:*:*:*:*:*:*:*:

cpe:2.3:h:ge:s2020:-:*:*:*:*:*:*:*:

cpe:2.3:h:ge:s2020g:-:*:*:*:*:*:*:*:

cpe:2.3:h:ge:s2020g:-:*:*:*:*:*:*:*:

cpe:2.3:o:ge:s2020g_firmware:*:*:*:*:*:*:*:*:

cpe:2.3:o:ge:s2020_firmware:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→