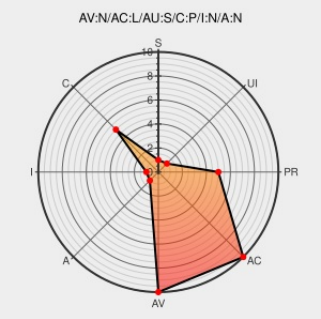
CVE-2014-8391

Published on: 06/02/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:51 PM UTC

CVE-2014-8391

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



Certain versions of Sendio from Sendio contain the following vulnerability:

The Web interface in Sendio before 7.2.4 does not properly handle sessions, which allows remote authenticated users to obtain sensitive information from other users' sessions via a large number of requests.

CVE-2014-8391 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4 - MEDIUM

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

CVE References

Description	Tags	Link
SecurityFocus	www.securityfocus.com text/html	BUGTRAQ 20150522 [CORE-2015-0010] - Sendio ESP Information Disclosure Vulnerability
Software Release History | Email Security and Efficiency – Sendio	Vendor Advisory www.sendio.com text/html	CONFIRM www.sendio.com/software-release-history/
Full Disclosure: [CORE-2015-0010] - Sendio ESP Information Disclosure Vulnerability	Exploit seclists.org text/html	FULLDISC 20150522 [CORE-2015-0010] - Sendio ESP Information Disclosure Vulnerability
Sendio ESP Information Disclosure ≈ Packet Storm	Exploit packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/132022/Sendio-ESP-Information-Disclosure.html
Sendio ESP - Information Disclosure	Exploit www.exploit-db.com	EXPLOIT-DB 37114

Proof of Concept

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
Application	Sendio	Sendio	All	All	All	All

cpe:2.3:a:sendio:sendio:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→