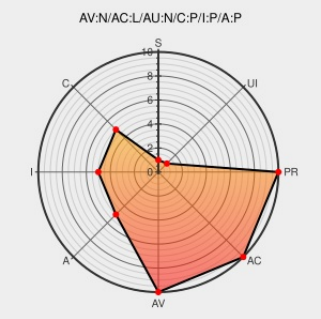
CVE-2005-2424

Published on: 08/03/2005 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:28 PM UTC

CVE-2005-2424

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



Certain versions of Santis 50 from Siemens contain the following vulnerability:

The management interface for Siemens SANTIS 50 running firmware 4.2.8.0, and possibly other products including Ericsson HN294dp and Dynalink RTA300W, allows remote attackers to access the Telnet port without authentication via certain packets to the web interface that cause the interface to freeze.

CVE-2005-2424 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
:: Secure Network :: Security Research Advisories.	Exploit, Vendor Advisory, web.archive.org, text/html, Inactive Link, Not Archived	MISC www.securenetwork.it/advisories/
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF santis50-packet-gain-access(21552)
Siemens Santis 50 Authentication Bypass Vulnerability - Advisories - Secunia	web.archive.org, text/html	SECUNIA 16215
Siemens Santis 50 Wireless Router Web Interface Denial Of Service Vulnerability	cve.report (archive), text/html	BID 14372

No Description Provided	www.osvdb.org Inactive Link Not Archived	OSVDB 18294
No Description Provided	marc.info text/html	BUGTRAQ 20050725 Siemens SANTIS 50 Authentication Vulnerability

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	Siemens	Santis 50	4.2.8.0	All	All	All
Hardware	Siemens	Santis 50	4.2.8.0	All	All	All

cpe:2.3:h:siemens:santis_50:4.2.8.0:*:*:*:*:*:*:*:

cpe:2.3:h:siemens:santis_50:4.2.8.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→