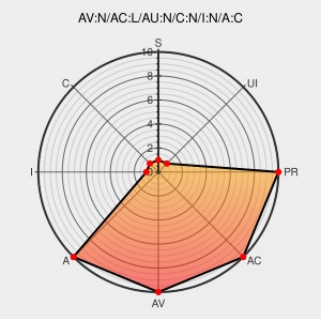
CVE-2003-1515

Published on: 12/31/2003 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:44 PM UTC

CVE-2003-1515

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



Certain versions of Asr-8100 from Origo contain the following vulnerability:

Origo ASR-8100 ADSL Router 3.21 has an administration service running on port 254 that does not require a password, which allows remote attackers to cause a denial of service by restoring the factory defaults.

CVE-2003-1515 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.8 - HIGH

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

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	XF origo-default-settings-restore(13463)
Origo ADSL Router Remote Administrative Interface Configuration Vulnerability	cve.report (archive) text/html	BID 8855
SecurityReason - Origo ASR-8100 ADSL router remote factory reset	Exploit securityreason.com text/html	SREASON 3300
SecurityFocus HOME Mailing List: BugTraq	Exploit www.securityfocus.com text/html	BUGTRAQ 20031012 Origo ASR-8100 ADSL router remote factory reset

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	Origo	Asr-8100	adsl_router_3.21	All	All	All
Hardware	Origo	Asr-8100	adsl_router_3.21	All	All	All
Hardware	Origo	Asr-8400	adsl_router	All	All	All
Hardware	Origo	Asr-8400	adsl_router	All	All	All

cpe:2.3:h:origo:asr-8100:adsl_router_3.21:*:*:*:*:*:*:*:

cpe:2.3:h:origo:asr-8100:adsl_router_3.21:*:*:*:*:*:*:*:

cpe:2.3:h:origo:asr-8400:adsl_router:*:*:*:*:*:*:*:

cpe:2.3:h:origo:asr-8400:adsl_router:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→