CVE-2017-16953

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-16953
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-12-01 17:29:00 UTC
Updated	2017-12-28 02:29:00 UTC
Description	connoppp.cgi on ZTE ZXDSL 831CII devices does not require HTTP Basic Authentication, which allows remote attackers to

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Zte	Zxdsl 831cii	-	All	All	All
Hardware	Zte	Zxdsl 831cii	-	All	All	All
Operating System	Zte	Zxdsl 831cii Firmware	-	All	All	All
Operating System	Zte	Zxdsl 831cii Firmware	-	All	All	All

References

Reference	Source	Link	Tags
ZTE ZXDSL 831 Unauthorized Configuration Access Bypass ≈ Packet Storm	MISC	packetstormsecurity.com	Exploit, Third P
ZTE ZXDSL 831CII - Improper Access Restrictions - Hardware webapps Exploit	EXPLOIT-DB	www.exploit-db.com	Third Party Adv
Security Bulletin Details	CONFIRM	support.zte.com.cn	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

Free CVE JSON API cve.report/api

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