CVE-2014-2651

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2014-2651
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-09 13:15:00 UTC
Updated	2020-01-21 21:00:00 UTC
Description	Unify OpenStage/OpenScape Desk Phone IP SIP before V3 R3.11.0 has an authentication bypass in the default mode of th

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Atos	Openscape Desk Phone Ip 35g	-	All	All	All
Hardware	Atos	Openscape Desk Phone Ip 35g	-	All	All	All
Hardware	Atos	Openscape Desk Phone Ip 35g Eco	-	All	All	All
Hardware	Atos	Openscape Desk Phone Ip 35g Eco	-	All	All	All
Operating System	Atos	Openscape Desk Phone Ip 35g Eco Firmware	v3	r3.11.0	All	All
Operating System	Atos	Openscape Desk Phone Ip 35g Eco Firmware	v3	r3.11.0	All	All
Operating System	Atos	Openscape Desk Phone Ip 35g Firmware	v3	r3.11.0	All	All
Operating System	Atos	Openscape Desk Phone Ip 35g Firmware	v3	r3.11.0	All	All
Hardware	Atos	Openscape Desk Phone Ip 55g	-	All	All	All
Hardware	Atos	Openscape Desk Phone Ip 55g	-	All	All	All
Operating System	Atos	Openscape Desk Phone Ip 55g Firmware	v3	r3.11.0	All	All
Operating System	Atos	Openscape Desk Phone Ip 55g Firmware	v3	r3.11.0	All	All
Hardware	Atos	Openstage 15	-	All	All	All
Hardware	Atos	Openstage 15	-	All	All	All
Operating System	Atos	Openstage 15 Firmware	v3	r3.11.0	All	All
Operating System	Atos	Openstage 15 Firmware	v3	r3.11.0	All	All
Hardware	Atos	Openstage 15 G	-	All	All	All

Hardware	Atos	Openstage 15 G	-	All	All	All
Operating System	Atos	Openstage 15 G Firmware	v3	r3.11.0	All	All
Operating System	Atos	Openstage 15 G Firmware	v3	r3.11.0	All	All
Hardware	Atos	Openstage 20	-	All	All	All
Hardware	Atos	Openstage 20	-	All	All	All
Hardware	Atos	Openstage 20 E	-	All	All	All
Hardware	Atos	Openstage 20 E	-	All	All	All
Operating System	Atos	Openstage 20 E Firmware	v3	r3.11.0	All	All
Operating System	Atos	Openstage 20 E Firmware	v3	r3.11.0	All	All
Operating System	Atos	Openstage 20 Firmware	v3	r3.11.0	All	All
Operating System	Atos	Openstage 20 Firmware	v3	r3.11.0	All	All
Hardware	Atos	Openstage 20 G	-	All	All	All
Hardware	Atos	Openstage 20 G	-	All	All	All
Operating System	Atos	Openstage 20 G Firmware	v3	r3.11.0	All	All
Operating System	Atos	Openstage 20 G Firmware	v3	r3.11.0	All	All
Hardware	Atos	Openstage 40	-	All	All	All
Hardware	Atos	Openstage 40	-	All	All	All
Operating System	Atos	Openstage 40 Firmware	v3	r3.11.0	All	All
Operating System	Atos	Openstage 40 Firmware	v3	r3.11.0	All	All
Hardware	Atos	Openstage 40 G	-	All	All	All
Hardware	Atos	Openstage 40 G	-	All	All	All
Operating System	Atos	Openstage 40 G Firmware	v3	r3.11.0	All	All
Operating System	Atos	Openstage 40 G Firmware	v3	r3.11.0	All	All
Hardware	Atos	Openstage 60	-	All	All	All
Hardware	Atos	Openstage 60	-	All	All	All
Operating System	Atos	Openstage 60 Firmware	v3	r3.11.0	All	All
Operating System	Atos	Openstage 60 Firmware	v3	r3.11.0	All	All
Hardware	Atos	Openstage 60 G	-	All	All	All
Hardware	Atos	Openstage 60 G	-	All	All	All
Operating System	Atos	Openstage 60 G Firmware	v3	r3.11.0	All	All
Operating System	Atos	Openstage 60 G Firmware	v3	r3.11.0	All	All
Hardware	Atos	Openstage 80	-	All	All	All
Hardware	Atos	Openstage 80	-	All	All	All
Operating System	Atos	Openstage 80 Firmware	v3	r3.11.0	All	All
Operating System	Atos	Openstage 80 Firmware	v3	r3.11.0	All	All

Hardware	Atos	Openstage 80 G	-	All	All	All
Hardware	Atos	Openstage 80 G	-	All	All	All
Operating System	Atos	Openstage 80 G Firmware	v3	r3.11.0	All	All
Operating System	Atos	Openstage 80 G Firmware	v3	r3.11.0	All	All

References

Reference	Source	Link	Tags
Unify Product Security Advisories and Security Notes | Unify	MISC	assets.yourcircuit.com	Third Party Advisory
networks.unify.com/security/advisories/OBSO-1403-02.pdf	MISC	networks.unify.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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