CVE-2020-24384

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-24384
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-10 14:15:00 UTC
Updated	2020-11-24 18:01:00 UTC
Description	A10 Networks ACOS and aGalaxy management Graphical User Interfaces (GUIs) have an unauthenticated Remote Code I

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	A10networks	Advanced Core Operating System	3.2.2	-	All	All
Operating System	A10networks	Advanced Core Operating System	3.2.2	p8	All	All
Operating System	A10networks	Advanced Core Operating System	3.2.3	-	All	All
Operating System	A10networks	Advanced Core Operating System	3.2.3	p5	All	All
Operating System	A10networks	Advanced Core Operating System	3.2.4	-	All	All
Operating System	A10networks	Advanced Core Operating System	3.2.4	p5	All	All
Operating System	A10networks	Advanced Core Operating System	3.2.5	-	All	All
Operating System	A10networks	Advanced Core Operating System	3.2.5	p1	All	All
Operating System	A10networks	Advanced Core Operating System	4.0.0	-	All	All
Operating System	A10networks	Advanced Core Operating System	4.0.1	p3	All	All
Operating System	A10networks	Advanced Core Operating System	4.1.0	-	All	All
Operating System	A10networks	Advanced Core Operating System	4.1.0	p13	All	All
Operating System	A10networks	Advanced Core Operating System	4.1.1	-	All	All
Operating System	A10networks	Advanced Core Operating System	4.1.1	p13	sp1	All
Operating System	A10networks	Advanced Core Operating System	4.1.100	-	All	All
Operating System	A10networks	Advanced Core Operating System	4.1.100	p7	All	All
Operating System	A10networks	Advanced Core Operating System	4.1.2	-	All	All

Operating System	A10networks	Advanced Core Operating System	4.1.2	p5	sp1	All
Operating System	A10networks	Advanced Core Operating System	4.1.4	-	All	All
Operating System	A10networks	Advanced Core Operating System	4.1.4	gr1-p4	sp1	All
Operating System	A10networks	Advanced Core Operating System	5.1.0	-	All	All
Operating System	A10networks	Advanced Core Operating System	5.1.0	p3	All	All
Operating System	A10networks	Advanced Core Operating System	3.2.2	-	All	All
Operating System	A10networks	Advanced Core Operating System	3.2.2	p8	All	All
Operating System	A10networks	Advanced Core Operating System	3.2.3	-	All	All
Operating System	A10networks	Advanced Core Operating System	3.2.3	p5	All	All
Operating System	A10networks	Advanced Core Operating System	3.2.4	-	All	All
Operating System	A10networks	Advanced Core Operating System	3.2.4	p5	All	All
Operating System	A10networks	Advanced Core Operating System	3.2.5	-	All	All
Operating System	A10networks	Advanced Core Operating System	3.2.5	p1	All	All
Operating System	A10networks	Advanced Core Operating System	4.0.0	-	All	All
Operating System	A10networks	Advanced Core Operating System	4.0.1	p3	All	All
Operating System	A10networks	Advanced Core Operating System	4.1.0	-	All	All
Operating System	A10networks	Advanced Core Operating System	4.1.0	p13	All	All
Operating System	A10networks	Advanced Core Operating System	4.1.1	-	All	All
Operating System	A10networks	Advanced Core Operating System	4.1.1	p13	sp1	All
Operating System	A10networks	Advanced Core Operating System	4.1.100	-	All	All
Operating System	A10networks	Advanced Core Operating System	4.1.100	p7	All	All
Operating System	A10networks	Advanced Core Operating System	4.1.2	-	All	All
Operating System	A10networks	Advanced Core Operating System	4.1.2	p5	sp1	All
Operating System	A10networks	Advanced Core Operating System	4.1.4	-	All	All
Operating System	A10networks	Advanced Core Operating System	4.1.4	gr1-p4	sp1	All
Operating System	A10networks	Advanced Core Operating System	5.1.0	-	All	All
Operating System	A10networks	Advanced Core Operating System	5.1.0	p3	All	All
Application	A10networks	Agalaxy	All	All	All	All
Application	A10networks	Agalaxy	3.0.1	All	All	All
Application	A10networks	Agalaxy	3.0.4	p3	All	All
Application	A10networks	Agalaxy	5.0.5	-	All	All
Application	A10networks	Agalaxy	All	All	All	All
Application	A10networks	Agalaxy	3.0.1	All	All	All
Application	A10networks	Agalaxy	3.0.4	p3	All	All
Application	A10networks	Agalaxy	5.0.5	-	All	All

Application	A10networks	Agalaxy	All	All	All	All

References

Reference	Source	Link	Tags
ACOS/aGalaxy GUI RCE Vulnerability – CVE-2020-24384 – A10 Support	CONFIRM	support.a10networks.com	Mitigation, Patch, Vendo
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.