



CVE-2020-24384

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

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 Execution (RCE) vulnerability. An attacker can exploit this vulnerability to execute arbitrary code on the affected system. The vulnerability is caused by a buffer overflow in the processing of untrusted input data.

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, Vendor			
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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

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