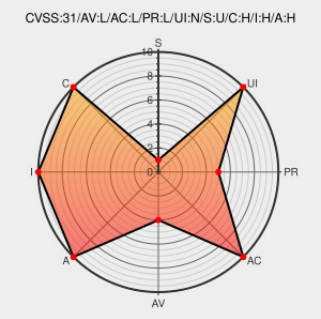
CVE-2019-14326

Published on: 04/14/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:58 PM UTC

CVE-2019-14326

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



Certain versions of Andy Os from Andyroid contain the following vulnerability:

An issue was discovered in AndyOS Andy versions up to 46.11.113. By default, it starts telnet and ssh (ports 22 and 23) with root privileges in the emulated Android system. This can be exploited by remote attackers to gain full access to the device, or by malicious apps installed inside the emulator to perform privilege escalation from a normal user to root (unlike with standard methods of getting root privileges on Android - e.g., the SuperSu program - the user is not asked for consent). There is no authentication performed - access to a root shell is given upon a successful connection. NOTE: although this was originally published with a slightly different CVE ID number, the correct ID for this Andy vulnerability has always been CVE-2019-14326.

CVE-2019-14326 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.2 - HIGH

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

CVE References

Description	Tags	Link
GitHub - seqred-s-a/cve-2019-14326: Privilege escalation in Andy emulator	Exploit Third Party Advisory github.com text/html	MISC github.com/seqred-s-a/cve-2019-14326
CVE-2019-14326 – privilege escalation in Andy | SEQRED	Exploit Third Party Advisory seqred.pl text/html	MISC seqred.pl/en/cve-privilege-escalation-in-andy/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, 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

Exploit/POC from Github

Privilege escalation in Andy emulator

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Andyroid	Andy Os	All	All	All	All

cpe:2.3:o:andyroid:andy_os:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

© CVE.report 2023 | |
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 registred 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