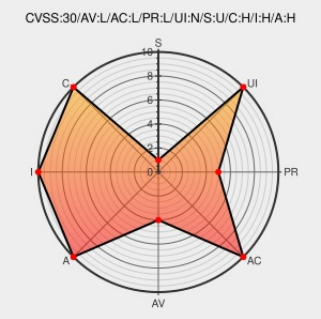
CVE-2017-16945

Published on: 01/31/2018 12:00:00 AM UTC

Last Modified on: 09/08/2021 05:21:00 PM UTC

CVE-2017-16945

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



Certain versions of Macos from Apple contain the following vulnerability:

The standardrestorer binary in Arq 5.10 and earlier for Mac allows local users to write to arbitrary files and consequently gain root privileges via a crafted restore path.

CVE-2017-16945 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
Mark Wadham	Third Party Advisory, m4.rkw.io, text/html	MISC m4.rkw.io/blog/two-local-root-privesc-bugs-in-arq-backup--510.html
Arq 5.10 - Local Privilege Escalation (2) -	Exploit	EXPLOIT-DB 43926

macOS local Exploit	Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	
Arq 5.10 Local Privilege Escalation ≈ Packet Storm	Exploit Third Party Advisory VDB Entry packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/146159/Arq-5.10-Local-Privilege-Escalation.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Apple	Macos	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Operating System	Apple	Mac Os	-	All	All	All
Application	Haystacksoftware	Arq	All	All	All	All

cpe:2.3:o:apple:macos:-:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os:-:*:*:*:*:*:*:*:

cpe:2.3:o:apple:mac_os:-:*:*:*:*:*:*:*:

cpe:2.3:a:haystacksoftware:arq:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→