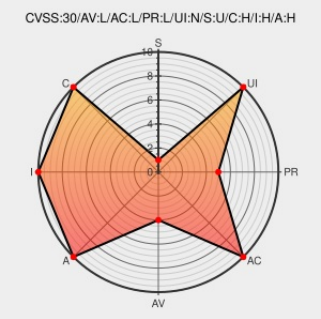
CVE-2019-14969

Published on: 08/12/2019 12:00:00 AM UTC

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

CVE-2019-14969

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



Certain versions of Auditor from Netwrix contain the following vulnerability:

Netwrix Auditor before 9.8 has insecure permissions on %PROGRAMDATA%\Netwrix Auditor\Logs\ActiveDirectory\ and sub-folders. In addition, the service Netwrix.ADA.StorageAuditService (which writes to that directory) does not perform proper impersonation, and thus the target file will have the same permissions as the invoking process (in this case, granting Authenticated Users full access over the target file). This vulnerability can be triggered by a low-privileged user to perform DLL Hijacking/Binary Planting attacks and ultimately execute code as NT AUTHORITY\SYSTEM with the help of Symbolic Links.

CVE-2019-14969 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: 6.9 - MEDIUM

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

CVE References

Description	Tags	Link
Advisories/ACTIVE-2019-010.md at master · active-labs/Advisories · GitHub	github.com text/html	MISC github.com/active-labs/Advisories/blob/master/2019/ACTIVE-2019-010.md

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netwrix	Auditor	All	All	All	All
Application	Netwrix	Auditor	All	All	All	All

cpe:2.3:a:netwrix:auditor:*:*:*:*:*:*:*:*:

cpe:2.3:a:netwrix:auditor:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→