CVE-2018-1127

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2018-1127
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-09-11 15:29:00 UTC
Updated	2019-10-09 23:38:00 UTC
Description	Tendrl API in Red Hat Gluster Storage before 3.4.0 does not immediately remove session tokens after a user logs out. Ses

Risk And Classification

Problem Types: CWE-384

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Redhat	Gluster Storage	All	All	All	All
Application	Redhat	Gluster Storage	All	All	All	All

References

Reference
Red Hat Customer Portal
Red Hat Gluster Storage Web Administration 'Tendrl-API' Session Caching Bug Lets Remote Users Hijack the Target User's Session - Securit
Fix caching issues for user APIs by shirshendu · Pull Request #422 · Tendrl/api · GitHub
1575835 – (CVE-2018-1127) CVE-2018-1127 tendrl-api: Improper cleanup of session token can allow attackers to hijack user sessions
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.