



CVE-2019-9867

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

Summary

CVE	CVE-2019-9867
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-03-21 16:01:00 UTC
Updated	2020-08-24 17:37:00 UTC
Description	An issue was discovered in the Web Console in Veritas NetBackup Appliance through 3.1.2. The proxy server password is

Risk And Classification

Problem Types: CWE-522

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Veritas	Netbackup Appliance	All	All	All	All

References

Reference	Source	Link	Tags
VTS19-001: Multiple Vulnerabilities in NetBackup Appliance Veritas™	MISC	www.veritas.com	Issue Tracking, Vendor
Veritas NetBackup Appliance Multiple Information Disclosure Vulnerabilities	BID	www.securityfocus.com	Third Party Advisory
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, 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](#)