CVE-2005-3327

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2005-3327
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-10-27 10:02:00 UTC
Updated	2016-10-18 03:34:00 UTC
Description	Network Appliance Data ONTAP 7.0 and earlier allows iSCSI Initiators to bypass iSCSI authentication via a modified client

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Network Appliance	Data Ontap	6.4	All	All	All
Application	Network Appliance	Data Ontap	6.5	All	All	All
Application	Network Appliance	Data Ontap	All	All	All	All
Application	Network Appliance	Data Ontap	6.4	All	All	All
Application	Network Appliance	Data Ontap	6.5	All	All	All
Application	Network Appliance	Data Ontap	All	All	All	All

References

Reference	Source	Link
Webmail - OVH	VUPEN	www.vupen.com
'Network Appliance iSCSI Authentication Bypass' - MARC	BUGTRAQ	marc.info
Secunia - Advisories - Network Appliance Data ONTAP iSCSI Authentication Bypass	SECUNIA	secunia.com
Network Appliance iSCSI Authentication Bypass Vulnerability	BID	www.securityfoc
www.matasano.com/advisories/netapp-iSCSI.txt	MISC	www.matasano.
SecurityTracker.com Archives - Network Appliance Data ONTAP iSCSI Security Controls Can Be Bypassed	SECTRACK	securitytracker.c
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**