CVE-2016-8612

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

Summary

CVE	CVE-2016-8612
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-09 20:29:00 UTC
Updated	2023-02-12 23:26:00 UTC
Description	Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol p

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	All	All	All	All
Application	Apache	Http Server	All	All	All	All
Application	Netapp	Storage Automation Store	-	All	All	All
Application	Netapp	Storage Automation Store	-	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All
Operating System	Redhat	Enterprise Linux	6.0	All	All	All
Operating System	Redhat	Enterprise Linux	7.0	All	All	All

References

Reference	Source	Link	T
1387605 – (CVE-2016-8612) CVE-2016-8612 JBCS mod_cluster: Protocol parsing logic error	CONFIRM	bugzilla.redhat.com	Is
Red Hat Customer Portal	REDHAT	access.redhat.com	T
Red Hat mod_cluster CVE-2016-8612 Denial of Service Vulnerability	BID	www.securityfocus.com	T
CVE-2016-8612 - Red Hat Customer Portal	MISC	access.redhat.com	
CVE-2016-8612 Apache HTTP Server Vulnerability in NetApp Products | NetApp Product Security	CONFIRM	security.netapp.com	T
Red Hat Customer Portal	REDHAT	access.redhat.com	T

Red Hat Customer Portal	MISC	access.redhat.com	
Red Hat Customer Portal	REDHAT	rhn.redhat.com	T
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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