CVE-2017-6633

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

Summary

CVE	CVE-2017-6633
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-22 01:29:00 UTC
Updated	2017-07-08 01:29:00 UTC
Description	A vulnerability in the TCP throttling process of Cisco UCS C-Series Rack Servers 3.0(0.234) could allow an unauthenticated

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Ucs C220 M4 Rack Server	-	All	All	All
Hardware	Cisco	Ucs C220 M4 Rack Server	-	All	All	All
Hardware	Cisco	Ucs C240 M4 Rack Server	-	All	All	All
Hardware	Cisco	Ucs C240 M4 Rack Server	-	All	All	All
Hardware	Cisco	Ucs C3160 Rack Server	-	All	All	All
Hardware	Cisco	Ucs C3160 Rack Server	-	All	All	All
Hardware	Cisco	Ucs C460 M4 Rack Server	-	All	All	All
Hardware	Cisco	Ucs C460 M4 Rack Server	-	All	All	All
Application	Cisco	Unified Computing System	3.0(0.234)	All	All	All
Application	Cisco	Unified Computing System	3.0\(0.234\)	All	All	All
Application	Cisco	Unified Computing System	3.0\(0.234\)	All	All	All

References

Reference
Cisco UCS C-Series Rack Servers TCP SYN Packet Throttling Bug Lets Remote Users Cause the Target Service to Stop Accepting New Con
Cisco UCS C-Series Rack Servers TCP Port Denial of Service Vulnerability
Cisco Unified Computing System C-Series Rack Servers CVE-2017-6633 Denial of Service Vulnerability

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.

Free CVE JSON API cve.report/api

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