



CVE-2019-1880

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

Summary

CVE	CVE-2019-1880
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-06-05 17:29:00 UTC
Updated	2019-10-09 23:48:00 UTC
Description	A vulnerability in the BIOS upgrade utility of Cisco Unified Computing System (UCS) C-Series Rack Servers could allow an

Risk And Classification

Problem Types: CWE-345

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Unified Computing System C125 M5	-	All	All	All
Hardware	Cisco	Unified Computing System C125 M5	-	All	All	All
Hardware	Cisco	Unified Computing System C220 M4	-	All	All	All
Hardware	Cisco	Unified Computing System C220 M4	-	All	All	All
Hardware	Cisco	Unified Computing System C220 M5	-	All	All	All
Hardware	Cisco	Unified Computing System C220 M5	-	All	All	All
Hardware	Cisco	Unified Computing System C240 M4	-	All	All	All
Hardware	Cisco	Unified Computing System C240 M4	-	All	All	All
Hardware	Cisco	Unified Computing System C240 M5	-	All	All	All
Hardware	Cisco	Unified Computing System C240 M5	-	All	All	All
Hardware	Cisco	Unified Computing System C460 M4	-	All	All	All
Hardware	Cisco	Unified Computing System C460 M4	-	All	All	All
Hardware	Cisco	Unified Computing System C480 M5	-	All	All	All
Hardware	Cisco	Unified Computing System C480 M5	-	All	All	All
Operating System	Cisco	Unified Computing System Server Firmware	All	All	All	All
Operating System	Cisco	Unified Computing System Server Firmware	All	All	All	All

References			
Reference	Source	Link	Ta
Cisco Unified Computing System Central Software CVE-2019-1880 Security Bypass Vulnerability	BID	www.securityfocus.com	
Cisco Unified Computing System BIOS Signature Bypass Vulnerability	CISCO	tools.cisco.com	Ve
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.			