



CVE-2013-4785

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2013-4785
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-07-08 22:55:00 UTC
Updated	2013-09-27 03:47:00 UTC
Description	The web interface on the Dell iDRAC6 with firmware before 1.95 allows remote attackers to modify the CLP interface for art

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Dell	Idrac6 Firmware	1.7	All	All	All
Operating System	Dell	Idrac6 Firmware	1.7	All	All	All

References

Reference	Source	Link
How to check if IPMI Cipher 0 is off - Systems Management - Wiki - Systems Management - Dell Community	MISC	en.community.de
ftp.dell.com/Manuals/Common/integrated-dell-remote-access-cntrlr-6-for-mo...	MISC	ftp.dell.com
All the IPMI that's fit to print	MISC	fish2.com
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.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

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](#)