



CVE-2018-1206

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

Summary

CVE	CVE-2018-1206
State	PUBLIC
Assigner	security_alert@emc.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-12 17:29:00 UTC
Updated	2018-04-13 14:51:00 UTC
Description	Dell EMC Data Protection Advisor versions prior to 6.3 Patch 159 and Dell EMC Data Protection Advisor versions prior to 6

Risk And Classification

Problem Types: CWE-798

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Emc	Data Protection Advisor	6.3.0	All	All	All
Application	Emc	Data Protection Advisor	6.4.0	All	All	All
Application	Emc	Data Protection Advisor	6.3.0	All	All	All
Application	Emc	Data Protection Advisor	6.4.0	All	All	All

References

Reference	Source	Link
Full Disclosure: DSA-2018-020: Dell EMC Data Protection Advisor Hardcoded Password Vulnerability	CONFIRM	seclists
EMC Data Protection Advisor Hardcoded Password Lets Local Users Gain Administrative Privileges - SecurityTracker	SECTrack	www.s
EMC Data Protection Advisor Local Hardcoded Credentials Information Disclosure Vulnerability	BID	www.s
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.ni

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)