



CVE-2016-6650

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

Summary

CVE	CVE-2016-6650
State	PUBLIC
Assigner	security_alert@emc.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-21 16:59:00 UTC
Updated	2017-07-12 01:29:00 UTC
Description	EMC RecoverPoint versions prior to 5.0 and EMC RecoverPoint for Virtual Machines versions prior to 5.0 have an SSL Stri

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Emc	Recoverpoint	All	All	All	All
Application	Emc	Recoverpoint For Virtual Machines	All	All	All	All

References

Reference	Source	Li
EMC RecoverPoint Flaw Lets Remote Users Conduct SSL Stripping Attacks to Access and Modify Data - SecurityTracker	SECTRACK	wv
EMC RecoverPoint SSL Stripping CVE-2016-6650 Security Bypass Vulnerability	BID	wv
SecurityFocus	CONFIRM	wv
CVE Program record	CVE.ORG	wv
NVD vulnerability detail	NVD	nv

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](#)