



CVE-2014-7288

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2014-7288
State	PUBLIC
Assigner	secure@symantec.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-02-01 02:59:00 UTC
Updated	2017-09-08 01:29:00 UTC
Description	Symantec PGP Universal Server and Encryption Management Server before 3.3.2 MP7 allow remote authenticated adminis

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Symantec	Encryption Management Server	All	mp6	All	All
Application	Symantec	Pgp Universal Server	All	mp6	All	All

References

Reference

- [Symantec Encryption Management Server Lets Local Users Gain Elevated Privileges and Remote Users Inject Email Headers - SecurityTrack](#)
- [Symantec Encryption Management Server CVE-2014-7288 Local Command Injection Vulnerability](#)
- [Symantec Encryption Management Server < 3.2.0 MP6 - Remote Command Injection](#)
- [IBM X-Force Exchange](#)
- [Security Advisories Relating to Symantec Products - Symantec Encryption Management Server Database Backup Command Line Injection ar](#)
- [117766](#)
- [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.

© [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](#)