



CVE-2013-4674

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

Summary

CVE	CVE-2013-4674
State	PUBLISHED
Assigner	symantec
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-07-31 13:20:28 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Cross-site scripting (XSS) vulnerability in the Web Email Protection component in Symantec Encryption Management Service

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

AV:N/AC:M/Au:N/C:N/I:P/A:N

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

AV:N/AC:M/Au:N/C:N/I:P/A:N

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Symantec	Encryption Management Server	3.3.0	All	All	All

Application	Symantec	Encryption Management Server	All	mp1	All	All
Application	Symantec	Pgp Universal Server	3.2.0	All	All	All
Application	Symantec	Pgp Universal Server	3.2.1	All	All	All
Application	Symantec	Pgp Universal Server	3.2.1	mp2	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference
Security Advisory SA54214 - Symantec Encryption Management Server Email Attachments Script Insertion Vulnerability - Secunia osvdb.org/95581
Symantec Encryption Management Server/PGP Universal Server Input Validation Flaw Permits Cross-Site Scripting Attacks - SecurityTracker
Security Advisories Relating to Symantec Products - Symantec Encryption Management Server Web Email Protection XSS - 2013-07-22T11:5
Symantec Encryption Management Server Web Email Protection Cross Site Scripting Vulnerability
IBM X-Force Exchange
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](#)