



# CVE-2014-2844

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

## Summary

<b>CVE</b>	CVE-2014-2844
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-04-18 14:55:00 UTC
<b>Updated</b>	2014-04-21 15:08:00 UTC
<b>Description</b>	Cross-site scripting (XSS) vulnerability in F-Secure Messaging Secure Gateway 7.5.0 before Patch 1862 allows remote aut

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	F-secure	Secure Messaging Secure Gateway	7.5.0	All	All	All
Application	F-secure	Secure Messaging Secure Gateway	7.5.0	All	All	All

## References

Reference	Source
Security Advisory SA58038 - F-Secure Messaging Security Gateway &quot;new&quot; Cross-Site Scripting Vulnerability - Secunia	SECUNIA
fsc-2014-2   F-Secure Labs	CONFIRMED
Full Disclosure: Reflected XSS Attacks vulnerabilities F-Secure Messaging Security Gateway V7.5.0.892 (CVE-2014-2844)	FULLDISCLOSURE
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#).

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

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