



CVE-2012-4596

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

Summary

CVE	CVE-2012-4596
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-08-22 10:42:00 UTC
Updated	2013-04-11 03:31:00 UTC
Description	Directory traversal vulnerability in McAfee Email Gateway (MEG) 7.0.0 and 7.0.1 allows remote authenticated users to bypass authentication and conduct cross-site scripting and directory traversal attacks.

Risk And Classification

Problem Types: CWE-22

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mcafee	Email Gateway	7.0.0	All	All	All
Application	Mcafee	Email Gateway	7.0.1	All	All	All
Application	Mcafee	Email Gateway	7.0.0	All	All	All
Application	Mcafee	Email Gateway	7.0.1	All	All	All

References

Reference
McAfee Email Gateway Lets Remote Users Bypass Authentication and Conduct Cross-Site Scripting and Directory Traversal Attacks - Security Bulletin
McAfee KnowledgeBase - McAfee Security Bulletin - EWS 5.5, 5.6, and MEG 7.0.1 hotfixes resolve multiple issues
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](#).

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