



CVE-2007-2957

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

Summary

CVE	CVE-2007-2957
State	PUBLISHED
Assigner	flexera
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-10-31 22:46:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	Integer overflow in McAfee E-Business Server before 8.5.3 for Solaris, and before 8.1.2 for Linux, HP-UX, and AIX, allows r

Risk And Classification

Primary CVSS: v2.0 9.3 from nvd@nist.gov

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

Problem Types: CWE-189 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Complete

Integrity

Complete

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Mcafee	E-business Server	All	All	aix	All

Application	Mcafee	E-business Server	All	All	hpux	All
Application	Mcafee	E-business Server	All	All	linux	All
Application	Mcafee	E-business Server	All	All	solaris	All

Vendor Declared Affected Products

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

References

Reference

knowledge.mcafee.com/SupportSite/dynamickc.do

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH

McAfee E-Business Server Authentication Packet Handling Integer Overflow Vulnerability

IBM X-Force Exchange

McAfee E-Business Server Authentication Packet Handling Buffer Overflow - Advisories - Secunia

McAfee E-Business Server Auth Packet Handling Buffer Overflow - Secunia Research - Secunia

McAfee E-Business Server Heap Overflow in Processing Authentication Packets Lets Remote Users Execute Arbitrary Code - SecurityTracke

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