



CVE-2007-4607

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

Summary

CVE	CVE-2007-4607
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-08-31 00:17:00 UTC
Updated	2018-08-28 17:29:00 UTC
Description	Buffer overflow in the EasyMailSMTPObj ActiveX control in emsmtp.dll 6.0.1 in the Quiksoft EasyMail SMTP Object, as use

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Gate Comm Software	Postcast Server Pro	3.0.61	All	All	All
Application	Gate Comm Software	Postcast Server Pro	3.0.61	All	All	All
Application	Quicksoft	Easymail Objects	All	All	All	All
Application	Quicksoft	Easymail Objects	All	All	All	All

References

Reference	Source
IBM X-Force Exchange	XF
VU#281977 - Quiksoft EasyMail SMTP ActiveX control stack buffer overflow vulnerabilities	CERT-VN
EasyMail Objects EMSMTP.DLL ActiveX Control Remote Buffer Overflow Vulnerability	BID
community.ivanti.com/docs/DOC-50988	MISC
EasyMail Objects IMAP4 and SMTP Components Buffer Overflows - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
20130424 Borland Caliber 11.0 Quiksoft EasyMail SMTP Object Buffer Overflows	BUGTRA
Postcast Server Pro 3.0.61 / Quiksoft EasyMail (emsmtp.dll 6.0.1) BoF	EXPLOIT
38335	OSVDB
Error 404 :(	MISC
PostCast Server EasyMail SMTP ActiveX Control Buffer Overflow - Advisories - Secunia	SECUNIA

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.	

© [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](#)