



CVE-2007-1029

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

Summary

CVE	CVE-2007-1029
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-02-21 11:28:00 UTC
Updated	2018-10-16 16:36:00 UTC
Description	Stack-based buffer overflow in the Connect method in the IMAP4 component in Quiksoft EasyMail Objects before 6.5 allow

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Quicksoft	Easymail Objects	All	All	All	All

References

Reference	Source
Risks in POS Systems: The Importance of a Security Assessment	MISC
SecurityFocus	BUGTRA
EasyMail Objects Connect Method Remote Stack Buffer Overflow Vulnerability	BID
EasyMail Objects IMAP4 and SMTP Components Buffer Overflows - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA
33208	OSVDB
IBM X-Force Exchange	XF
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
CXSecurity - IDS	SREASC
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](#)