



Vulnerability Advisory

Name	EasyMail Objects EasyMail IMAP v6.5 Connect Method Stack Overflow
Date Released	February 16, 2007
Affected Software	EasyMail Objects Prior v6.5
Researcher	Paul Craig paul.craig@security-assessment.com

Description

During a security review of the safe-for-scripting EasyMail objects, a stack overflow was discovered in the connect method of EasyMail IMAP4 (Object ClassID {703B353E-FA2E-4072-8DDF-F70AAC7E527E})

Exploitation

When the object is initialized and the Connect method is called, a stack overflow is possible when a large (500+ characters) host name is specified. Once arbitrary data has been written to the stack, it is possible to overflow the structured exception handler and gain command execution.

Solution

Security-Assessment.com has been in contact with Quiksoft and a new version of the software has been released to address the discovered vulnerability.

Security-Assessment.com urges EasyMail users to upgrade to the latest version which is available at <http://www.quiksoft.com/download/emsetup.exe>.

About Security-Assessment.com

Security-Assessment.com is Australasia's leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

Security-Assessment.com is an Endorsed Commonwealth Government of Australia supplier and sits on the Australian Government Attorney-General's Department Critical Infrastructure Project panel. We are certified by both Visa and MasterCard under their Payment Card Industry Data Security Standard Programs. For further information on this issue or any of our service offerings, contact us

Web www.security-assessment.com
Email info@security-assessment.com
Phone +649 302 5093

