



CVE-2004-2466

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

Summary

CVE	CVE-2004-2466
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-12-31 05:00:00 UTC
Updated	2022-08-01 17:15:00 UTC
Description	chat.ghp in Easy Chat Server 1.2 allows remote attackers to cause a denial of service (server crash) via a long username p

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Efs Software	Easy Chat Server	1.2	All	All	All
Application	Efs Software	Easy Chat Server	2.2	All	All	All
Application	Efs Software	Easy Chat Server	1.2	All	All	All
Application	Efs Software	Easy Chat Server	2.2	All	All	All

References

Reference	Source	Link
20040702 Multiple Vulnerabilities in Easy Chat Server 1.2	FULLDISC	archives.nec
Security Advisory SA58427 - Easy Chat Server "username" Buffer Overflow Vulnerability - Secunia	SECUNIA	secunia.com
IBM X-Force Exchange	XF	exchange.xf
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.
Easy Chat Server "username" Buffer Overflow Vulnerability - Advisories - Secunia	SECUNIA	secunia.com
Easy Chat Server 3.1 - Stack Buffer Overflow	EXPLOIT-DB	www.exploit-
Secunia - Advisories - Easy Chat Server Multiple Vulnerabilities	SECUNIA	secunia.com
Neohapsis Archives - Bugtraq - #0013 - Multiple Vulnerabilities in Easy Chat Server 1.2	BUGTRAQ	archives.nec
IBM X-Force Exchange	XF	exchange.xf
404 Not Found	MISC	www.autistic

EFS Software Easy Chat Server Authentication Request Handling Remote Buffer Overflow Vulnerability	BID	www.securit
Easy Chat Server 3.1 Buffer Overflow ≈ Packet Storm	MISC	packetstorm
Easy Chat Server Stack-Based Buffer Overflow Vulnerability	BID	www.securit
7416	OSVDB	www.osvdb.
EFS Easy Chat Server 2.2 - Remote Denial of Service - Windows dos Exploit	EXPLOIT-DB	www.exploit-
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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