



CVE-2008-1502

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

Summary

CVE	CVE-2008-1502
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-03-25 19:44:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	The _bad_protocol_once function in phpgwapi/inc/class.kses.inc.php in KSES, as used in eGroupWare before 1.4.003, Mo

Risk And Classification

Primary CVSS: v2.0 4.3 from nvd@nist.gov

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

Problem Types: CWE-79 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

Partial

Availability

None

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Egroupware	Egroupware	1.0	All	All	All

Application	Egroupware	Egroupware	1.0.1	All	All	All
Application	Egroupware	Egroupware	1.0.3	All	All	All
Application	Egroupware	Egroupware	1.0.6	All	All	All
Application	Egroupware	Egroupware	1.2.106-2	All	All	All
Application	Egroupware	Egroupware	1.4.001	All	All	All
Application	Egroupware	Egroupware	All	All	All	All
Application	Moodle	Moodle	1.1.1	All	All	All
Application	Moodle	Moodle	1.2.0	All	All	All
Application	Moodle	Moodle	1.2.1	All	All	All
Application	Moodle	Moodle	1.3.0	All	All	All
Application	Moodle	Moodle	1.3.1	All	All	All
Application	Moodle	Moodle	1.3.2	All	All	All
Application	Moodle	Moodle	1.3.3	All	All	All
Application	Moodle	Moodle	1.3.4	All	All	All
Application	Moodle	Moodle	1.4.1	All	All	All
Application	Moodle	Moodle	1.4.2	All	All	All
Application	Moodle	Moodle	1.4.3	All	All	All
Application	Moodle	Moodle	1.4.4	All	All	All
Application	Moodle	Moodle	1.4.5	All	All	All
Application	Moodle	Moodle	1.5	All	All	All
Application	Moodle	Moodle	1.5.0	beta	All	All
Application	Moodle	Moodle	1.5.1	All	All	All
Application	Moodle	Moodle	1.5.2	All	All	All
Application	Moodle	Moodle	1.5.3	All	All	All
Application	Moodle	Moodle	1.6.0	All	All	All
Application	Moodle	Moodle	1.6.1	All	All	All
Application	Moodle	Moodle	1.6.2	All	All	All
Application	Moodle	Moodle	1.6.3	All	All	All
Application	Moodle	Moodle	1.6.4	All	All	All
Application	Moodle	Moodle	1.6.5	All	All	All
Application	Moodle	Moodle	1.6.6	All	All	All
Application	Moodle	Moodle	1.6.7	All	All	All
Application	Moodle	Moodle	1.7.1	All	All	All
Application	Moodle	Moodle	1.7.2	All	All	All
Application	Moodle	Moodle	1.7.3	All	All	All
Application	Moodle	Moodle	1.7.4	All	All	All

Application	Moodle	Moodle	1.7.5	All	All	All
Application	Moodle	Moodle	1.7.6	All	All	All
Application	Moodle	Moodle	1.8.1	All	All	All
Application	Moodle	Moodle	1.8.2	All	All	All
Application	Moodle	Moodle	1.8.3	All	All	All
Application	Moodle	Moodle	All	All	All	All
Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		
References						
Reference				Source		
Fedora update for moodle - Secunia Advisories - Vulnerability Intelligence - Secunia.com				af854a3a-2127-422b-91ae-3		
Moodle KSES HTML Filter Bypass Vulnerability - Advisories - Secunia				af854a3a-2127-422b-91ae-3		
USN-658-1: Moodle vulnerability Ubuntu security notices				af854a3a-2127-422b-91ae-3		
SUSE Update for Multiple Packages - Secunia Advisories - Vulnerability Intelligence - Secunia.com				af854a3a-2127-422b-91ae-3		
oss-security - Re: CVE request: moodle xss in < 1.8.5				af854a3a-2127-422b-91ae-3		
eGroupWare HTML Filter Bypass Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com				af854a3a-2127-422b-91ae-3		
Debian -- Security Information -- DSA-1691-1 moodle				af854a3a-2127-422b-91ae-3		
Ubuntu update for moodle - Secunia Advisories - Vulnerability Intelligence - Secunia.com				af854a3a-2127-422b-91ae-3		
[security-announce] SUSE Security Summary Report SUSE-SR:2008:015				af854a3a-2127-422b-91ae-3		
Gentoo update for egroupware - Secunia Advisories - Vulnerability Intelligence - Secunia.com				af854a3a-2127-422b-91ae-3		
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH				af854a3a-2127-422b-91ae-3		
Moodle KSES HTML Filter Bypass Vulnerability - Secunia Advisories - Vulnerability Intelligence - Secunia.com				af854a3a-2127-422b-91ae-3		
www.egroupware.org/viewvc/branches/1.4/phpgwapi/inc/class.kses.inc.php				af854a3a-2127-422b-91ae-3		
Ubuntu update for moodle - Secunia Advisories - Vulnerability Intelligence - Secunia.com				af854a3a-2127-422b-91ae-3		
eGroupWare: Multiple vulnerabilities — Gentoo Linux Documentation				af854a3a-2127-422b-91ae-3		
IBM X-Force Exchange				af854a3a-2127-422b-91ae-3		
Latest release notes - MoodleDocs				af854a3a-2127-422b-91ae-3		
Debian -- Security Information -- DSA-1871-1 wordpress				af854a3a-2127-422b-91ae-3		
[SECURITY] Fedora 8 Update: moodle-1.8.5-1.fc8				af854a3a-2127-422b-91ae-3		
RETIRED: eGroupWare ' _bad_protocol_once()' HTML Security Bypass Vulnerability				af854a3a-2127-422b-91ae-3		
egroupware.org: ChangeLog EPL/CE 14.1				af854a3a-2127-422b-91ae-3		
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](#)