



CVE-2005-2665

Published on: 08/23/2005 12:00:00 AM UTC

Last Modified on: 02/13/2023 01:09:26 AM UTC

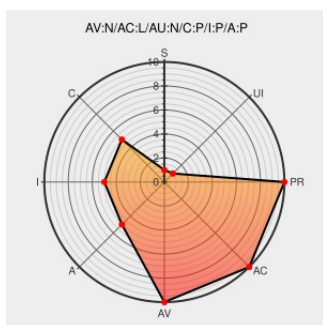
CVE-2005-2665

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Elm](#) from [Elm Development Group](#) contain the following vulnerability:

Stack-based buffer overflow in expires.c in Elm 2.5 PL5 through PL7, and possibly other versions, allows remote attackers to execute arbitrary code via an e-mail message with a long Expires header.

CVE-2005-2665 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

PARTIAL

PARTIAL

PARTIAL

CVE References

Description

Tags

Link

Secunia - Advisories - ELM "Expires" Header Parsing Buffer Overflow Vulnerability

[web.archive.org](#)
[text/html](#)

[SECUNIA 16508](#)

SecurityTracker.com Archives - Elm Buffer Overflow in SMTP 'Expires' Header Lets Remote Users Execute Arbitrary Code

[Patch](#)
[securitytracker.com](#)
[text/html](#)

[SECTRACK 1014745](#)

'ELM < 2.5.8 Remote Exploit POC' - MARC

[marc.info](#)
[text/x-c](#)

[BUGTRAQ 20050822 ELM < 2.5.8 Remote Exploit POC](#)

Neohapsis Archives - Full Disclosure List - #0688 - [Full-disclosure] [RETRO AUDITING] Elm remote buffer overflow in Expires header

[Patch](#)
[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[FULLDISC 20050820 \[RETRO AUDITING\] Elm remote buffer overflow in Expires header](#)

Gentoo Linux Documentation -- Lynx: Buffer overflow in NNTP processing

[www.gentoo.org](#)
[text/html](#)

[GENTOO GLSA-200510-15](#)

Advisories - Mandriva	www.mandriva.com text/html	 MANDRIVA MDKSA-2005:186
The Slackware Linux Project: Slackware Security Advisories	www.slackware.org text/html	 SLACKWARE SSA:2005-310-03
Elm Expires Header Remote Buffer Overflow Vulnerability	cve.report (archive) text/html	 BID 14613
Lynx NNTP Article Header Buffer Overflow Vulnerability	cve.report (archive) text/html	 BID 15117
Malformed Request	www.securityfocus.com text/html Inactive Link Not Archived	 SCO SA-2005.47
The Slackware Linux Project: Slackware Security Advisories	www.slackware.org text/html	 SLACKWARE SSA:2005-311
Secunia - Advisories - Red Hat update for elm	web.archive.org text/html	 SECUNIA 16554
Secunia - Advisories - Slackware update for elm	web.archive.org text/html	 SECUNIA 17475

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Elm Development Group	Elm	2.5_pl5	All	All	All
Application	Elm Development Group	Elm	2.5_pl6	All	All	All
Application	Elm Development Group	Elm	2.5_pl7	All	All	All
Application	Elm Development Group	Elm	2.5_pl5	All	All	All
Application	Elm Development Group	Elm	2.5_pl6	All	All	All
Application	Elm Development Group	Elm	2.5_pl7	All	All	All

```
cpe:2.3:a:elm development group:elm:2.5 pl5:*.**:*.**:.*
```

```
cpe:2.3:a:elm development group:elm:2.5 pl6:*.:.:.:.:.:
```

```
cpe:2.3:a:elm_development_group:elm:2.5 pl7:*.:.:.:.:.:
```

```
cpe:2.3:a:elm development group:elm:2.5 pl5:*.***.***.***.
```

```
cpe:2.3:a:elm development group:elm:2.5 pl6:*.***.***.***.
```

cpe:2.3:a:elm_development_group:elm:2.5_pl/:*:~::~:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

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](#)