



# CVE-2007-5034

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2007-5034
<b>State</b>	PUBLIC
<b>Assigner</b>	security@ubuntu.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2007-09-21 20:17:00 UTC
<b>Updated</b>	2018-10-15 21:40:00 UTC
<b>Description</b>	ELinks before 0.11.3, when sending a POST request for an https URL, appends the body and content headers of the POST

## Risk And Classification

**Problem Types:** CWE-200

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Elinks</a>	<a href="#">Elinks</a>	All	All	All	All
Application	<a href="#">Elinks</a>	<a href="#">Elinks</a>	All	All	All	All

## References

Reference	Source	Link
ELinks HTTPS POST Request Information Disclosure Weakness	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
[SECURITY] Fedora Core 6 Update: elinks-0.11.3-1.fc6	FEDORA	<a href="http://www.redhat.com">www.redhat.com</a>
USN-519-1: elinks vulnerability   Ubuntu	UBUNTU	<a href="http://www.ubuntu.com">www.ubuntu.com</a>
rPath update for elinks - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
[SECURITY] Fedora 7 Update: elinks-0.11.3-1.fc7	FEDORA	<a href="http://www.redhat.com">www.redhat.com</a>
ELinks Proxy CONNECT Weakness - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
297981 – CVE-2007-5034 elinks reveals POST data to HTTPS proxy [F7]	CONFIRM	<a href="http://bugzilla.redhat.com">bugzilla.redhat.com</a>
Debian -- Security Information -- DSA-1380-1 elinks	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
Fedora update for elinks - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Repository / Oval Repository	OVAL	<a href="http://oval.cisecurity.org">oval.cisecurity.org</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>
SecurityTracker.com Archives - ELinks May Disclose POST Request Data in Clear Text to Remote Users	SECTRACK	<a href="http://www.securitytracker.com">www.securitytracker.com</a>

Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>
403 Forbidden	CONFIRM	<a href="http://bugzilla.elinks.cz">bugzilla.elinks.cz</a>
Fedora update for elinks - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	<a href="http://secunia.com">secunia.com</a>
SecurityFocus	BUGTRAQ	<a href="http://www.securityfocus">www.securityfocus</a>
Red Hat update for elinks - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Bug #141018 "ELinks reveals POST data to HTTPS proxy" : Bugs : elinks package : Ubuntu	CONFIRM	<a href="http://bugs.launchpad.net">bugs.launchpad.net</a>
Ubuntu update for elinks - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Debian update for elinks - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](http://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](http://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](http://www.mitre.org). This site includes MITRE data granted under the following [license](http://www.mitre.org).

**CVE.report and Source URL Uptime Status [status.cve.report](http://status.cve.report)**