



# CVE-2004-1267

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

## Summary

<b>CVE</b>	CVE-2004-1267
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2005-01-10 05:00:00 UTC
<b>Updated</b>	2018-10-03 21:29:00 UTC
<b>Description</b>	Buffer overflow in the ParseCommand function in hppl-input.c in the hppltops program for CUPS 1.1.22 allows remote attac

## Risk And Classification

### Problem Types: CWE-119

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.0.4	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.0.4_8	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.1	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.10	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.12	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.13	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.14	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.15	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.16	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.17	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.18	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.19	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.19_rc5	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.20	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.21	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.22_rc1	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.4	All	All	All

Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.4_2	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.4_3	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.4_5	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.6	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.7	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.0.4	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.0.4_8	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.1	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.10	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.12	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.13	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.14	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.15	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.16	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.17	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.18	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.19	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.19_rc5	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.20	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.21	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.22_rc1	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.4	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.4_2	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.4_3	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.4_5	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.6	All	All	All
Application	<a href="#">Easy Software Products</a>	<a href="#">Cups</a>	1.1.7	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Fedora Core</a>	core_2.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Fedora Core</a>	core_3.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Fedora Core</a>	core_2.0	All	All	All
Operating System	<a href="#">Redhat</a>	<a href="#">Fedora Core</a>	core_3.0	All	All	All

## References

Reference	Source	Link	Tags
Advisories - Mandriva	MANDRAKE	<a href="http://www.mandriva.com">www.mandriva.com</a>	

404 Not Found	MISC	<a href="https://tigger.uic.edu">tigger.uic.edu</a>	Exploit, Vendor Advisory
Gentoo Linux Documentation -- CUPS: Multiple vulnerabilities	GENTOO	<a href="https://www.gentoo.org">www.gentoo.org</a>	
<a href="https://rhn.redhat.com">rhn.redhat.com</a>   Red Hat Support	REDHAT	<a href="https://www.redhat.com">www.redhat.com</a>	
USN-50-1: CUPS vulnerabilities   Ubuntu security notices	UBUNTU	<a href="https://usn.ubuntu.com">usn.ubuntu.com</a>	
IBM X-Force Exchange	XF	<a href="https://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>	
<a href="https://rhn.redhat.com">rhn.redhat.com</a>   Red Hat Support	REDHAT	<a href="https://www.redhat.com">www.redhat.com</a>	
Repository / Oval Repository	OVAL	<a href="https://oval.cisecurity.org">oval.cisecurity.org</a>	
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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

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