



# CVE-2004-0148

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

## Summary

<b>CVE</b>	CVE-2004-0148
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2004-04-15 04:00:00 UTC
<b>Updated</b>	2018-05-03 01:29:00 UTC
<b>Description</b>	wu-ftpd 2.6.2 and earlier, with the restricted-gid option enabled, allows local users to bypass access restrictions by changing

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Sgi</a>	<a href="#">Propack</a>	2.3	All	All	All
Application	<a href="#">Sgi</a>	<a href="#">Propack</a>	2.4	All	All	All
Application	<a href="#">Sgi</a>	<a href="#">Propack</a>	2.3	All	All	All
Application	<a href="#">Sgi</a>	<a href="#">Propack</a>	2.4	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.1	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18	All	academ	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr10	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr11	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr12	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr13	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr14	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr15	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr4	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr5	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr6	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr7	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr8	All	All	All

Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr9	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta2	All	academ	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_vr16	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_vr17	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.5.0	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.6.0	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.6.1	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.6.2	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.1	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18	All	academ	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr10	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr11	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr12	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr13	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr14	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr15	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr4	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr5	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr6	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr7	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr8	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta18_vr9	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_beta2	All	academ	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_vr16	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.4.2_vr17	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.5.0	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.6.0	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.6.1	All	All	All
Application	<a href="#">Washington University</a>	<a href="#">Wu-ftpd</a>	2.6.2	All	All	All

## References

Reference	Source	Link
Debian -- Security Information -- DSA-457-1 wu-ftpd	DEBIAN	<a href="http://www.debian.org">www.debian.org</a>
redhat.com   Red Hat Support	REDHAT	<a href="http://www.redhat.com">www.redhat.com</a>
Repository / Oval Repository	OVAL	<a href="http://oval.cisecurity.org">oval.cisecurity.org</a>

Felicitations ! Votre domaine a bien ete cree chez OVH !	FHSIRI	<a href="http://www.trisirt.com">www.trisirt.com</a>
Secunia - Advisories - WU-FTPD Directory Access Restriction Bypass Vulnerability	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Repository / Oval Repository	OVAL	<a href="http://oval.cisecurity.o">oval.cisecurity.o</a>
Repository / Oval Repository	OVAL	<a href="http://oval.cisecurity.o">oval.cisecurity.o</a>
Repository / Oval Repository	OVAL	<a href="http://oval.cisecurity.o">oval.cisecurity.o</a>
IBM X-Force Exchange	XF	<a href="http://exchange.xforce">exchange.xforce</a>
'[security bulletin] SSRT4704 rev.0 HP-UX wu-ftpd local unauthorized access' - MARC	HP	<a href="http://marc.info">marc.info</a>
Solaris in.ftpd Directory Access Restriction Bypass Vulnerability - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
#102356: Security Vulnerability in the Solaris 9 in.ftpd(1M) Server May Allow Unauthorized Directory Access	SUNALERT	<a href="http://sunsolve.sun.co">sunsolve.sun.co</a>
WU-FTPD restricted-gid Unauthorized Access Vulnerability	BID	<a href="http://www.securityfoc">www.securityfoc</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://The MITRE Corporation) and the authoritative source of CVE content is [MITRE's CVE web site](http://MITRE's CVE web site). This site includes MITRE data granted under the following [license](http://license).

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