



CVE-2008-5692

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

Summary

CVE	CVE-2008-5692
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-12-19 18:30:00 UTC
Updated	2018-10-11 20:56:00 UTC
Description	Ipswitch WS_FTP Server Manager before 6.1.1, and possibly other Ipswitch products, allows remote attackers to bypass au

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ipswitch	Ws Ftp	1.0.5	All	All	All
Application	Ipswitch	Ws Ftp	2.01	All	All	All
Application	Ipswitch	Ws Ftp	2.02	All	All	All
Application	Ipswitch	Ws Ftp	2.03	All	All	All
Application	Ipswitch	Ws Ftp	3.0	All	All	All
Application	Ipswitch	Ws Ftp	3.0.1	All	All	All
Application	Ipswitch	Ws Ftp	3.1.0	All	All	All
Application	Ipswitch	Ws Ftp	3.1.1	All	All	All
Application	Ipswitch	Ws Ftp	3.1.2	All	All	All
Application	Ipswitch	Ws Ftp	3.1.3	All	All	All
Application	Ipswitch	Ws Ftp	3.14	All	All	All
Application	Ipswitch	Ws Ftp	4.00	All	All	All
Application	Ipswitch	Ws Ftp	4.01	All	All	All
Application	Ipswitch	Ws Ftp	4.02	All	All	All
Application	Ipswitch	Ws Ftp	5.00	All	All	All
Application	Ipswitch	Ws Ftp	5.01	All	All	All
Application	Ipswitch	Ws Ftp	5.02	All	All	All

Application	Ipswitch	Ws Ftp	5.03	All	All	All
Application	Ipswitch	Ws Ftp	5.04	All	All	All
Application	Ipswitch	Ws Ftp	5.05	All	All	All
Application	Ipswitch	Ws Ftp	6.0	All	All	All
Application	Ipswitch	Ws Ftp	1.0.5	All	All	All
Application	Ipswitch	Ws Ftp	2.01	All	All	All
Application	Ipswitch	Ws Ftp	2.02	All	All	All
Application	Ipswitch	Ws Ftp	2.03	All	All	All
Application	Ipswitch	Ws Ftp	3.0	All	All	All
Application	Ipswitch	Ws Ftp	3.0.1	All	All	All
Application	Ipswitch	Ws Ftp	3.1.0	All	All	All
Application	Ipswitch	Ws Ftp	3.1.1	All	All	All
Application	Ipswitch	Ws Ftp	3.1.2	All	All	All
Application	Ipswitch	Ws Ftp	3.1.3	All	All	All
Application	Ipswitch	Ws Ftp	3.14	All	All	All
Application	Ipswitch	Ws Ftp	4.00	All	All	All
Application	Ipswitch	Ws Ftp	4.01	All	All	All
Application	Ipswitch	Ws Ftp	4.02	All	All	All
Application	Ipswitch	Ws Ftp	5.00	All	All	All
Application	Ipswitch	Ws Ftp	5.01	All	All	All
Application	Ipswitch	Ws Ftp	5.02	All	All	All
Application	Ipswitch	Ws Ftp	5.03	All	All	All
Application	Ipswitch	Ws Ftp	5.04	All	All	All
Application	Ipswitch	Ws Ftp	5.05	All	All	All
Application	Ipswitch	Ws Ftp	6.0	All	All	All
Application	Ipswitch	Ws Ftp	All	All	All	All

References

Reference	Source	Link
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	www.vupen.com
IPSwitch WS_FTP Server Manager Security Bypass - Secunia Advisories - Vulnerability Intelligence - Secunia.com	SECUNIA	secunia.com
aluigi.altervista.org/adv/wsftpweblog-adv.txt	MISC	aluigi.altervista.org
SecurityFocus	BUGTRAQ	www.securityfocus.com
Release Notes for WS_FTP Server 6.1.1 and WS_FTP Server 6.1.1 with SSH	CONFIRM	docs.ipswitch.com
WS_FTP Server Manager Authentication Bypass and Information Disclosure Vulnerabilities	BID	www.securityfocus.com
CVS - WS_FTP Server Manager Authentication Bypass and Information Disclosure Vulnerabilities	CONFIRM	www.securityfocus.com

CXSecurity - IDS	SREASON	securityre
SecurityFocus	BUGTRAQ	www.secu
CVE Program record	CVE.ORG	www.cve.o
NVD vulnerability detail	NVD	nvd.nist.g

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)