CVE-2006-0705

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2006-0705
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-02-15 11:06:00 UTC
Updated	2017-07-20 01:29:00 UTC
Description	Format string vulnerability in a logging function as used by various SFTP servers, including (1) AttachmateWRQ Reflection

Risk And Classification

Problem Types: CWE-134

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Attachmatewrq	Reflection For Secure It Server	6.0	All	unix	All
Application	Attachmatewrq	Reflection For Secure It Server	6.0	All	win	All
Application	Attachmatewrq	Reflection For Secure It Server	6.0	All	unix	All
Application	Attachmatewrq	Reflection For Secure It Server	6.0	All	win	All
Application	F-secure	F-secure Ssh Server	3.0.0	All	All	All
Application	F-secure	F-secure Ssh Server	3.0.1	All	All	All
Application	F-secure	F-secure Ssh Server	3.0.1	All	unix	All
Application	F-secure	F-secure Ssh Server	3.0.2	All	All	All
Application	F-secure	F-secure Ssh Server	3.0.3	All	All	All
Application	F-secure	F-secure Ssh Server	3.0.4	All	All	All
Application	F-secure	F-secure Ssh Server	3.0.5	All	All	All
Application	F-secure	F-secure Ssh Server	3.0.6	All	All	All
Application	F-secure	F-secure Ssh Server	3.0.7	All	All	All
Application	F-secure	F-secure Ssh Server	3.0.8	All	All	All
Application	F-secure	F-secure Ssh Server	3.0.9	All	All	All
Application	F-secure	F-secure Ssh Server	3.1.0	All	All	All
Application	F-secure	F-secure Ssh Server	3.1.0	All	unix	All

Application	F-secure	F-secure Ssh Server	3.1.0_build9	All	All	All
Application	F-secure	F-secure Ssh Server	3.2.0	All	unix	All
Application	F-secure	F-secure Ssh Server	3.2.3	All	unix	All
Application	F-secure	F-secure Ssh Server	5.0	All	All	All
Application	F-secure	F-secure Ssh Server	5.1	All	win	All
Application	F-secure	F-secure Ssh Server	5.2	All	win	All
Application	F-secure	F-secure Ssh Server	5.3	All	win	All
Application	F-secure	F-secure Ssh Server	3.0.0	All	All	All
Application	F-secure	F-secure Ssh Server	3.0.1	All	All	All
Application	F-secure	F-secure Ssh Server	3.0.1	All	unix	All
Application	F-secure	F-secure Ssh Server	3.0.2	All	All	All
Application	F-secure	F-secure Ssh Server	3.0.3	All	All	All
Application	F-secure	F-secure Ssh Server	3.0.4	All	All	All
Application	F-secure	F-secure Ssh Server	3.0.5	All	All	All
Application	F-secure	F-secure Ssh Server	3.0.6	All	All	All
Application	F-secure	F-secure Ssh Server	3.0.7	All	All	All
Application	F-secure	F-secure Ssh Server	3.0.8	All	All	All
Application	F-secure	F-secure Ssh Server	3.0.9	All	All	All
Application	F-secure	F-secure Ssh Server	3.1.0	All	All	All
Application	F-secure	F-secure Ssh Server	3.1.0	All	unix	All
Application	F-secure	F-secure Ssh Server	3.1.0_build9	All	All	All
Application	F-secure	F-secure Ssh Server	3.2.0	All	unix	All
Application	F-secure	F-secure Ssh Server	3.2.3	All	unix	All
Application	F-secure	F-secure Ssh Server	5.0	All	All	All
Application	F-secure	F-secure Ssh Server	5.1	All	win	All
Application	F-secure	F-secure Ssh Server	5.2	All	win	All
Application	F-secure	F-secure Ssh Server	5.3	All	win	All

References

Reference
Webmail - OVH
WRQ Reflection Secure IT SFTP Format String Vulnerability - Advisories - Secunia
Gentoo net-misc/ssh Vulnerability - Advisories - Secunia
Webmail - OVH
SSH Communications Security's Secure Shell Server: SFTP privilege escalation — Gentoo Linux Documentation

IBM X-Force Exchange
US-CERT Vulnerability Note VU#419241
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
AttachmateWRQ Reflection for Secure IT Remote Format String Vulnerability
HP Tru64 UNIX SSH SFTP Server Vulnerability - Advisories - Secunia
HPSBTU02322
SSH Tectia Server SFTP Service Unspecified Vulnerability - Advisories - Secunia
SSH Tectia Server Remote Format String Vulnerability
SecurityTracker.com Archives - SSH Tectia Server SFTP Logging Bug May Let Remote Authenticated Users Execute Arbitrary Commands
WRQ Tech Note 1882 - Reflection for Secure IT Server Security Vulnerability Update and Workaround
CVE Program record
NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status **status.cve.report**