



CVE-2004-0930

Published on: 11/19/2004 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:11 PM UTC

CVE-2004-0930

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Linux](#) from [Conectiva](#) contain the following vulnerability:

The ms_fnmatch function in Samba 3.0.4 and 3.0.7 and possibly other versions allows remote authenticated users to cause a denial of service (CPU consumption) via a SAMBA request that contains multiple * (wildcard) characters.

CVE-2004-0930 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

NONE

Integrity
Impact

NONE

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

Security Announcement

[web.archive.org](#)

[text/html](#)

[Inactive Link](#) [Not Archived](#)

[ot SUSE SUSE-SA:2004:040](#)

usn/usn-22-1 - Ubuntu Linux

[www.ubuntu.com](#)

[text/html](#)

[UBUNTU USN-22-1](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)

[text/html](#)

[XF samba-msfnmatch-dos\(17987\)](#)

Samba Remote Wild Card Denial Of Service Vulnerability

[Patch](#)

[Vendor Advisory](#)

[cve.report \(archive\)](#)

[text/html](#)

[BID 11624](#)

Home - Conectiva

[distro.conectiva.com.br](#)

[text/html](#)

[CONECTIVA CLA-2004:899](#)

'[OpenPKG-SA-2004.054] OpenPKG Security Advisory (samba)' - MARC	marc.info text/html	 OPENPKG OpenPKG-SA-2004.054
APPLE-SA-2005-03-21 Security Update 2005-003	lists.apple.com text/html	 APPLE APPLE-SA-2005-03-21
Repository / Oval Repository	oval.cisecurity.org text/html	 OVAL oval:org.mitre.oval:def:10936
Accenture Let there be change	Exploit Patch Vendor Advisory www.idefense.com text/html	 IDeFENSE 20041108 Samba SMBD Remote Denial of Service Vulnerability
Advisories - Mandriva	www.mandriva.com text/html	 MANDRAKE MDKSA-2004:131
No Description Provided	patches.sgi.com Inactive Link Not Archived	 SGI 20041201-01-P
'[SECURITY] CAN-2004-0930: Potential Remote Denial of Service Vulnerability' - MARC	marc.info text/html	 BUGTRAQ 20041108 [SECURITY] CAN-2004-0930: Potential Remote Denial of Service Vulnerability
#101783: Security Vulnerability in Samba's "ms_fnmatch()" Function May Result in a Denial of Service (DoS)	web.archive.org text/html Inactive Link Not Archived	 SUNALERT 101783
	ftp.sco.com text/plain	 SCO SCOSA-2005.17
Gentoo Linux Documentation -- Samba: Multiple vulnerabilities	www.gentoo.org text/html	 GENTOO GLSA 200411-21
By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.		

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Conectiva	Linux	10.0	All	All	All
Operating System	Conectiva	Linux	10.0	All	All	All
Operating System	Gentoo	Linux	All	All	All	All
Operating System	Gentoo	Linux	All	All	All	All
Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server_ia64	All

System						
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server_ia64	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation_ia64	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	workstation_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	advanced_server_ia64	All
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	2.1	All	enterprise_server_ia64	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation	All
Operating System	Redhat	Enterprise Linux	2.1	All	workstation_ia64	All
Operating System	Redhat	Enterprise Linux	3.0	All	advanced_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	enterprise_server	All
Operating System	Redhat	Enterprise Linux	3.0	All	workstation_server	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Enterprise Linux Desktop	3.0	All	All	All
Operating System	Redhat	Fedora Core	core_2.0	All	All	All
Operating System	Redhat	Fedora Core	core_3.0	All	All	All
Operating System	Redhat	Fedora Core	core_2.0	All	All	All
Operating System	Redhat	Fedora Core	core_3.0	All	All	All
Operating	Redhat	Linux Advanced Workstation	2.1	All	ia64	All

ΟΡΓΑΝΩΣΗ

```
cpe:2.3:o:gentoo:linux:*:*:*:*:*:*:*:
```

```
cpe:2.3:o:gentoo:linux:*:*:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux:2.1:*:advanced_server:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux:2.1:*:advanced_server:ia64:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux:2.1:*:enterprise_server:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux:2.1:*:enterprise_server:ia64:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux:2.1:*:workstation:*:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise_linux:2.1:*:workstation ia64:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise linux:3.0:*:advanced server:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise linux:3.0:*:enterprise server:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise_linux:3.0:*:workstation_server:*:*:*.*:
```

```
cpe:2.3:o:redhat:enterprise_linux:2.1:*:advanced_server:*:*:*.*.*
```

```
cpe:2.3:o:redhat:enterprise_linux:2.1:*:advanced_server:ia64:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise linux:2.1:*:enterprise server:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise_linux:2.1:*:enterprise_server:ia64:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux:2.1:*:workstation:*:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise_linux:2.1:*:workstation_ia64:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux:3.0:*:advanced_server:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise linux:3.0:*:enterprise server:*:*:*:*
```

```
cpe:2.3:o:redhat:enterprise_linux:3.0:*:workstation_server:*:*:*.*:
```

```
cpe:2.3:o:redhat:enterprise_linux_desktop:3.0:*:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:enterprise_linux_desktop:3.0:*:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:fedora_core:core_2.0:*:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:fedora_core:core 3.0:*:*:*:*:*:*
```

```
cpe:2.3:o:redhat:fedora_core:core_2.0:*:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:fedora_core:core_3.0:*:*:*:*:*:
```

```
cpe:2.3:o:redhat:linux_advanced_workstation:2.1:*:ia64:*:*:*:*:
```

```
cpe:2.3:o:redhat:linux advanced workstation:2.1:*:itanium processor:*.*.*.*.:
```

cpe:2.3:o:redhat:linux_advanced_workstation:2.1:*:ia64:*:*:*:*:
cpe:2.3:o:redhat:linux_advanced_workstation:2.1:*:itanium_processor:*:*:*:*:
cpe:2.3:a:samba:samba:3.0.0:*:*:*:*:*:
cpe:2.3:a:samba:samba:3.0.3:*:*:*:*:*:
cpe:2.3:a:samba:samba:3.0.4:*:*:*:*:*:
cpe:2.3:a:samba:samba:3.0.5:*:*:*:*:*:
cpe:2.3:a:samba:samba:3.0.6:*:*:*:*:*:
cpe:2.3:a:samba:samba:3.0.7:*:*:*:*:*:
cpe:2.3:a:samba:samba:3.0.0:*:*:*:*:*:
cpe:2.3:a:samba:samba:3.0.3:*:*:*:*:*:
cpe:2.3:a:samba:samba:3.0.4:*:*:*:*:*:
cpe:2.3:a:samba:samba:3.0.5:*:*:*:*:*:
cpe:2.3:a:samba:samba:3.0.6:*:*:*:*:*:
cpe:2.3:a:samba:samba:3.0.7:*:*:*:*:*:
cpe:2.3:a:sgi:samba:3.0:*:irix:*:*:*:*:
cpe:2.3:a:sgi:samba:3.0.1:*:irix:*:*:*:*:
cpe:2.3:a:sgi:samba:3.0.2:*:irix:*:*:*:*:
cpe:2.3:a:sgi:samba:3.0.3:*:irix:*:*:*:*:
cpe:2.3:a:sgi:samba:3.0.4:*:irix:*:*:*:*:
cpe:2.3:a:sgi:samba:3.0.5:*:irix:*:*:*:*:
cpe:2.3:a:sgi:samba:3.0.6:*:irix:*:*:*:*:
cpe:2.3:a:sgi:samba:3.0.7:*:irix:*:*:*:*:
cpe:2.3:a:sgi:samba:3.0:*:irix:*:*:*:*:
cpe:2.3:a:sgi:samba:3.0.1:*:irix:*:*:*:*:
cpe:2.3:a:sgi:samba:3.0.2:*:irix:*:*:*:*:
cpe:2.3:a:sgi:samba:3.0.3:*:irix:*:*:*:*:
cpe:2.3:a:sgi:samba:3.0.4:*:irix:*:*:*:*:
cpe:2.3:a:sgi:samba:3.0.5:*:irix:*:*:*:*:

cpe:2.3:a:sgi:samba:3.0.6:*:irix:*:*:*:*:

cpe:2.3:a:sgi:samba:3.0.7:*:irix:*:*:*:*:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)

© [CVE.report](#) 2023   |

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](#)