

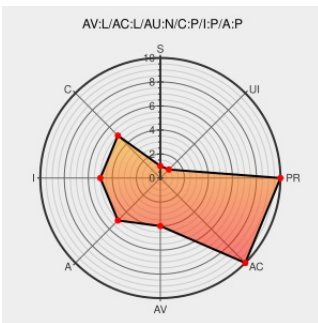


CVE-2004-1948

Published on: 04/20/2004 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:09 PM UTC

CVE-2004-1948

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

Certain versions of [Ncftp](#) from [Ncftp Software](#) contain the following vulnerability:

NcFTP client 3.1.6 and 3.1.7, when the username and password are included in an FTP URL that is provided on the command line, allows local users to obtain sensitive information via "ps aux," which displays the URL in the process list.

CVE-2004-1948 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.6 - MEDIUM**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

NcFTP Local Information Disclosure Vulnerability

[Vendor Advisory](#)
[cve.report \(archive\)](#)
[text/html](#)

[BID 10182](#)

No Description Provided

[www.osvdb.org](#)

[OSVDB 5595](#)

Inactive Link Not Archived

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF ncftp-info-disclosure\(15919\)](#)

Secunia - Advisories - NcFTP Client Password Leakage Security Issue

[Exploit](#)
[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)

[SECUNIA 11438](#)

'NcFTP - password leaking' - MARC

[marc.info](#)

[BUGTRAQ 20040419 NcFTP -](#)

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ncftp Software	Ncftp	3.0.0	All	All	All
Application	Ncftp Software	Ncftp	3.0.1	All	All	All
Application	Ncftp Software	Ncftp	3.0.2	All	All	All
Application	Ncftp Software	Ncftp	3.0.3	All	All	All
Application	Ncftp Software	Ncftp	3.0.4	All	All	All
Application	Ncftp Software	Ncftp	3.1.0	All	All	All
Application	Ncftp Software	Ncftp	3.1.1	All	All	All
Application	Ncftp Software	Ncftp	3.1.2	All	All	All
Application	Ncftp Software	Ncftp	3.1.3	All	All	All
Application	Ncftp Software	Ncftp	3.1.4	All	All	All
Application	Ncftp Software	Ncftp	3.1.5	All	All	All
Application	Ncftp Software	Ncftp	3.1.6	All	All	All
Application	Ncftp Software	Ncftp	3.1.7	All	All	All
Application	Ncftp Software	Ncftp	3.0.0	All	All	All
Application	Ncftp Software	Ncftp	3.0.1	All	All	All
Application	Ncftp Software	Ncftp	3.0.2	All	All	All
Application	Ncftp Software	Ncftp	3.0.3	All	All	All
Application	Ncftp Software	Ncftp	3.0.4	All	All	All
Application	Ncftp Software	Ncftp	3.1.0	All	All	All
Application	Ncftp Software	Ncftp	3.1.1	All	All	All
Application	Ncftp Software	Ncftp	3.1.2	All	All	All
Application	Ncftp Software	Ncftp	3.1.3	All	All	All
Application	Ncftp Software	Ncftp	3.1.4	All	All	All
Application	Ncftp Software	Ncftp	3.1.5	All	All	All
Application	Ncftp Software	Ncftp	3.1.6	All	All	All
Application	Ncftp Software	Ncftp	3.1.7	All	All	All

[illegible]

```
cpe:2.3:a:ncip_software:ncip:3.0.0::: : : : : : : :
```

```
cpe:2.3:a:ncftp_software:ncftp:3.0.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:ncftp_software:ncftp:3.0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:ncftp_software:ncftp:3.0.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:ncftp_software:ncftp:3.0.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:ncftp_software:ncftp:3.1.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:ncftp_software:ncftp:3.1.1:*:*:*:*:*:*:
```

```
cpe:2.3:a:ncftp_software:ncftp:3.1.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:ncftp_software:ncftp:3.1.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:ncftp_software:ncftp:3.1.4:*:*:*:*:*:
```

```
cpe:2.3:a:ncftp_software:ncftp:3.1.5:*:*:*:*:*:
```

```
cpe:2.3:a:ncftp_software:ncftp:3.1.6:*:*:*:*:*:
```

```
cpe:2.3:a:ncftp_software:ncftp:3.1.7:::~::~:
```

```
cpe:2.3:a:ncftp_software:ncftp:3.0.0:*:*:*:*:*:*:
```

```
cpe:2.3:a:ncftp_software:ncftp:3.0.1:::~::~:
```

```
cpe:2.3:a:ncftp_software:ncftp:3.0.2:*:*:*:*:*:*:
```

```
cpe:2.3:a:ncftp_software:ncftp:3.0.3:*:*:*:*:*:*:
```

```
cpe:2.3:a:ncftp_software:ncftp:3.0.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:ncftp_software:ncftp:3.1.0:*:*:*:*:*:
```

```
cpe:2.3:a:ncftp_software:ncftp:3.1.1:*:*:*:*:*:
```

```
cpe:2.3:a:ncftp:software:ncftp:3.1.2:*:*:*:*:*:
```

```
cpe:2.3:a:ncftp:software:ncftp:3.1.3:*:*:*:*:*:
```

```
cpe:2.3:a:ncftp_software:ncftp:3.1.4:*:*:*:*:*:*:
```

```
cpe:2.3:a:ncftp_software:ncftp:3.1.5:*:*:*:*:*:
```

```
cpe:2.3:a:ncftp_software:ncftp:3.1.6:*:*:*:*:*:
```

```
cpe:2.3:a:ncftp_software:ncftp:3.1.7:*:*:*:*:*:
```

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](#)