快速通道

文档分类
- 软件作品
- 文档作品 <=
- 代码作品

推荐作品
- 对 RPC DCOM worm 的设想
- [vulnwatch] Serv-U MDTM Command Buffer Overflow Vulnerab...

[vulnwatch] Serv-U MDTM Command Buffer Overflow Vulnerability

提交作品： bkbll
提交日期： 2004-02-29
作品属性： 推荐
文档类别： 文档作品
相关下载： **=>下载<=**
浏览次数： 今1次/总3974次

---

vulnwatch] Serv-U MDTM Command Buffer Overflow Vulnerability

www.cnhonker.com
Security Advisory

Advisory Name: Serv-U MDTM Command Buffer Overflow Vulnerability
Release Date: 02/26/2004
Affected version: Serv-U < 5.0.0.4
Author: bkbll <bkbll@cnhonker.net>
URL: http://www.cnhonker.com/advisory/serv-u.mdtm.txt
Overview:

The Serv-U is a ftp daemon runs on windows. Serv-U supports a ftp command "MDTM" \
for user changing file time . There is a buffer overflow when a user logged in and \
send a malformed time zone as MDTM argument. This can be remote exploit and gain \
SYSTEM privilege.

Exploit:

When a user logged in, he can send this
MDTM
20031111111111+AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA /test.txt
You must have a valid user account and password to exploit it, and you are not \
need WRITE or any other privilege. And even the test.txt,which is the file you \
request, can not be there. :) So you can put your shellcode as the filename.

About HUC:

HUC is still alive.

返回上页

Copyright © 2000-2004 **HUC** All Rights Reserved.