

# [NEWS] 4D WebSTAR Multiple Vulnerabilities

**Source:** <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0048.html>

---

**From:** SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

**Date:** 07/14/04

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 14 Jul 2004 10:24:59 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

## 4D WebSTAR Multiple Vulnerabilities

---

### SUMMARY

4D WebSTAR is a software product that provides Web, FTP, and Mail services for Mac OS X. There are numerous vulnerabilities that allow for an attacker to escalate privileges or obtain access to protected resources.

### DETAILS

#### Vulnerable Systems:

- \* WebSTAR version 5.3.2 and prior

#### Immune Systems:

- \* WebSTAR version 5.3.3

#### Issue #1: Remotely Exploitable Pre-Authentication FTP overflow

There is a stack based buffer overflow within the FTP service. An attacker can take advantage of this overflow by sending in a long FTP command. This can happen prior to authentication. A long FTP command will trigger a stack based memory trespass. Upon successful exploitation, an attacker will have the privileges of the 'webstar' user and group id 'wheel'. An attacker can gain administrative privileges by taking advantage of Issue #4.

## Securiteam: [NEWS] 4D WebSTAR Multiple Vulnerabilities

### Issue #2: Directory Indexing of Any Directory on Host

One of the sample scripts included with WebSTAR (/cgi-bin/ShellExample.cgi) can be used to gain a directory listing of any directory on the server. This is done by sending in a path to the directory followed by an asterisk ("\*") as the query string. Issue

### #3: File Disclosure of PHP.INI

There is a vulnerability within the WebServer that allows an attacker to download the php.ini files located within the /cgi-bin and /fcgi-bin directories. This can contain sensitive information about the WebServer and the Database Server, potentially including the account and password used by PHP to communicate with the database.

### Issue #4: Local Privilege Escalation and File Overwrite Via Symbolic Links

WebSTAR will attempt to open up files via a relative path from the current working directory. An attacker can use this vulnerability to overwrite files with the private key of the WebServer. Due to a default umask that creates files with global read and write privileges, an attacker create files related to the cron subsystem that will allow a local attacker to obtain administrative privileges.

### Disclosure Timeline:

Vendor notified: 04/05/2004

Fix available: 07/08/2004

Advisory released: 07/13/2004

### Vendor Response:

4D has released an upgrade for 4D WebSTAR. Download WebSTAR 5.3.3:

[ftp://ftp.4d.com/products/webstar/current/4d\\_webstar\\_v/4d\\_webstar\\_v.sit](ftp://ftp.4d.com/products/webstar/current/4d_webstar_v/4d_webstar_v.sit)

[ftp://ftp.4d.com/products/webstar/current/4d\\_webstar\\_v/4d\\_webstar\\_v.sit](ftp://ftp.4d.com/products/webstar/current/4d_webstar_v/4d_webstar_v.sit)

### Bug Fix information [URL wraps]:

[ftp://ftp.4d.com/ACI\\_PRODUCT\\_REFERENCE\\_LIBRARY/4D\\_PRODUCT\\_DOCUMENTATION/PDF\\_Docs\\_by](ftp://ftp.4d.com/ACI_PRODUCT_REFERENCE_LIBRARY/4D_PRODUCT_DOCUMENTATION/PDF_Docs_by)

[ftp://ftp.4d.com/ACI\\_PRODUCT\\_REFERENCE\\_LIBRARY/4D\\_PRODUCT\\_DOCUMENTATION/PDF\\_Docs by 4](ftp://ftp.4d.com/ACI_PRODUCT_REFERENCE_LIBRARY/4D_PRODUCT_DOCUMENTATION/PDF_Docs_by)

### ADDITIONAL INFORMATION

The information has been provided by <mailto:advisories@atstake.com>  
@Stake Advisories.

The original article can be found at:

<<http://www.atstake.com/research/advisories/2004/a071302-1.txt>>

<http://www.atstake.com/research/advisories/2004/a071302-1.txt>

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

Securiteam: [NEWS] 4D WebSTAR Multiple Vulnerabilities

=====  
=====

**DISCLAIMER:**

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.