

# [VulnWatch] @stake advisory: 4D WebSTAR Multiple Vulnerabilities

**Source:** <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2004-07/0005.html>

---

**From:** Advisories ([advisories\\_at\\_atstake.com](mailto:advisories_at_atstake.com))

**Date:** 07/13/04

Date: Tue, 13 Jul 2004 11:47:25 -0400

To: <[vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)>

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

@stake, Inc.

[www.atstake.com](http://www.atstake.com)

Security Advisory

Advisory Name: WebSTAR 5.3.2 Multiple Vulnerabilities

Release Date: 07/13/2004

Application: WebSTAR 5.3.2 and below

Platform: MacOS X 10.3.3 and below

Severity: A remote attacker can obtain root privileges

A remote attacker can get directory listings of  
any directory

A remote attacker can obtain copies of the PHP  
configuration file

A local attacker can obtain root privileges

Author: Dave G. <[daveg@atstake.com](mailto:daveg@atstake.com)>

Vendor Status: Upgrade with fix available

CVE Candidate: Candidate number applied for

Reference: [www.atstake.com/research/advisories/2004/a071302-1.txt](http://www.atstake.com/research/advisories/2004/a071302-1.txt)

## Overview:

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:

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.

## VulnWatch: [VulnWatch] @stake advisory: 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)

Bug Fix information [URL wraps]:

[ftp://ftp.4d.com/ACI\\_PRODUCT\\_REFERENCE\\_LIBRARY/4D\\_PRODUCT\\_DOCUMENTATION/PDF\\_Docs\\_by\\_4D\\_Product\\_A-Z/4D\\_WebSTAR/Software\\_Change\\_History.txt](ftp://ftp.4d.com/ACI_PRODUCT_REFERENCE_LIBRARY/4D_PRODUCT_DOCUMENTATION/PDF_Docs_by_4D_Product_A-Z/4D_WebSTAR/Software_Change_History.txt)

### @stake Recommendation:

Upgrade to WebSTAR 5.3.3.

### Common Vulnerabilities and Exposures (CVE) Information:

The Common Vulnerabilities and Exposures (CVE) project has assigned the following names to these issues. These are candidates for inclusion in the CVE list (<http://cve.mitre.org>), which standardizes names for security problems.

Candidate number applied for.

@stake Vulnerability Reporting Policy:

<http://www.atstake.com/research/policy/>

@stake Advisory Archive:

<http://www.atstake.com/research/advisories/>

PGP Key:

[http://www.atstake.com/research/pgp\\_key.asc](http://www.atstake.com/research/pgp_key.asc)

Copyright 2004 @stake, Inc. All rights reserved.

-----BEGIN PGP SIGNATURE-----

VulnWatch: [VulnWatch] @stake advisory: 4D WebSTAR Multiple Vulnerabilities

Version: PGP 8.0.3

iQA/AwUBQPQDAke9kNifAm4yEQLXfQCg9RmGtwSW+WZ0/VnNu5rLi9L4RHEAoP3d  
PDIFu044IqX9Mb4FmyJcTYiQ

=zlii

-----END PGP SIGNATURE-----