

[Full-Disclosure] iDEFENSE Security Advisory 11.08.02a: File Disclosure Vulnerability in Simple Web Server

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2002-11/0074.html>

From: David Endler (dendler@idefense.com)

Date: 11/08/02

From: dendler@idefense.com (David Endler)

Date: Fri, 8 Nov 2002 15:27:16 -0500

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

Hash: SHA1

iDEFENSE Security Advisory 11.08.02a:

<http://www.idefense.com/advisory/11.08.02a.txt>

File Disclosure Vulnerability in Simple Web Server

November 8, 2002

I. BACKGROUND

As its name suggests, Peter Sandvik's Simple Web Server is a Linux-based web server. More information about it is available at <http://www.linuxstuffs.cjb.net>.

II. DESCRIPTION

Restricted files can be remotely accessed because of Simple Web Server's failure to properly handle malformed URL requests for said files. For example, if a standard URL to access a restricted file is <http://server.com/secret/file>, the altered URL <http://server.com///secret/file> will bypass any access control on that file, thereby granting unauthorized access to it.

III. ANALYSIS

The resulting damage from accessing restricted files on the web server is dependent on the actual file accessed and what kind of information is contained within. Simple Web Server is not a widely distributed web server, according to Netcraft.com. As such, the likelihood of widespread exploitation is unlikely.

IV. DETECTION

Simple Web Server 0.5.1, running on Red Hat Linux 7.3, is vulnerable. The vulnerability does not seem to be platform-specific, since it works on Debian Linux 3.0 as well.

V. WORKAROUND

Migrate to other supported web servers, being the software is no longer actively maintained.

VI. VENDOR RESPONSE

Peter Sandvik said he will suspend work on the project for now, being he "doesn't have time to work on it."

VII. CVE INFORMATION

The Mitre Corp.'s Common Vulnerabilities and Exposures (CVE) Project assigned the identification number CAN-2002-1238 to this issue.

VIII. DISCLOSURE TIMELINE

08/29/2002 Issue disclosed to iDEFENSE
09/25/2002 Maintainer, Peter Sandvik notified
09/25/2002 iDEFENSE clients notified
09/25/2002 Response received from Peter Sandvik
(peter.sandvik@home.se)
09/26/2002 Started e-mail discussions regarding status of software support
10/31/2002 Last e-mail received regarding status of software support
11/08/2002 Public disclosure

IX. CREDIT

Tamer Sahin (ts@securityoffice.net) discovered this vulnerability.

Get paid for security research
<http://www.idefense.com/contributor.html>

Subscribe to iDEFENSE Advisories:
send email to listserv@idefense.com, subject line: "subscribe"

About iDEFENSE:

iDEFENSE is a global security intelligence company that proactively monitors sources throughout the world — from technical vulnerabilities and hacker profiling to the global spread of viruses and other malicious code. Our security intelligence services provide decision-makers, frontline security professionals and network administrators with timely access to actionable intelligence and decision support on cyber-related threats. For more information, visit <http://www.idefense.com>.

--dave

David Endler, CISSP
Director, Technical Intelligence
iDEFENSE, Inc.
14151 Newbrook Drive
Suite 100
Chantilly, VA 20151
voice: 703-344-2632
fax: 703-961-1071

dendler@idefense.com
www.idefense.com

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

Version: PGP 7.1.2

Comment: <http://pgp.mit.edu:11371/pks/lookup?op=get&search=0x4B0ACC2A>

iQA/AwUBPcwdxUrdNYRLCswqEQLB3wCfauM7/75ebKpsA70fmHN2I1t2fGMAoNra
anqP0AHYTOkh4K5MJnsLXywG
=Dx3m

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