

[NEWS] IBM Infoprint Remote Management DoS

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-10/0128.html>

From: support@securiteam.com

Date: 10/25/02

From: support@securiteam.com

To: list@securiteam.com

Date: 25 Oct 2002 15:41:41 +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

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> -- Know that you're safe.

IBM Infoprint Remote Management DoS

SUMMARY

<<http://www.printers.ibm.com/R5PSC.NSF/Web/wglaserselect>> IBM makes a series of TCP/IP enabled printers that come with remote management features. One of these features is a Telnet-based remote management service, which has a DoS vulnerability. The vulnerability discussed here was tested on an IBM Infoprint 21 (older model), but is probably present in other printers of the same product line.

DETAILS

The Telnet-enabled remote management feature used in the printer does not properly check user input, namely the login name. By connecting to port 23 and entering a login name consisting of an excessive number of characters a DoS condition will occur, and the Telnet service will refuse to allow further logins to the service. This is most likely due to a buffer overflow vulnerability in the login handling code.

Power cycling the printer will restore functionality.

Impact:

After the DoS condition has occurred, the Telnet service on the printer will continue accepting connections but will no longer display a login prompt. The connection will eventually time out. Other services are

Securiteam: [NEWS] IBM Infoprint Remote Management DoS

unaffected.

While testing with large input data Toni Lassila was able to bring the entire printer down hard by sending enough data (several k) to port 23. The entire network interface was down, and the physical control panel on the printer was unresponsive. Printing was not possible. The only solution was to power cycle the printer once or twice(!) to restore functionality.

Workaround:

There do not appear to be any firmware updates available for the specific printer, nor any mention of these types of issues on the vendor's web site. Best practices dictate that printers and other internal assets should be only accessible from the internal network or through authenticated connections.

It does not seem to be possible to disable the Telnet service without disabling all TCP/IP functionality from the printer.

Vendor Status:

IBM was contacted on 2002-10-18. No acknowledgement of response of any kind was received.

ADDITIONAL INFORMATION

The information has been provided by <mailto:toni.lassila@mc-europe.com>
Toni Lassila.

=====

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.

-
- **Previous message:** support@securiteam.com: "[TOOL] Opticon|Users, Display Currently Logged-on Users on Your Windows Network"
 - **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)