

[NEWS] Multiple Vulnerabilities with Pingtel xpressa SIP Phones

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-07/0050.html>

From: support@securiteam.com

Date: 07/12/02

From: support@securiteam.com

To: list@securiteam.com

Date: Fri, 12 Jul 2002 19:40:52 +0200 (CEST)

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.

Multiple Vulnerabilities with Pingtel xpressa SIP Phones

SUMMARY

Pingtel develops intelligent Java-based voice-over-IP phones for service providers and enterprises. The vulnerabilities discussed in this advisory were found using Pingtel's xpressa voice-over-IP phones model PX-1 software versions 1.2.5-1.2.7.4.

The Pingtel xpressa SIP-based phone contains multiple vulnerabilities affecting all aspects of the phone's operation. These vulnerabilities include remote access to the phone; remote administrative access to the phone; manipulation of SIP signaling; multiple denials of service; remote telnet access (complete control of the VxWorks operating system); local physical administrative access, and more.

Using the vulnerabilities enumerated within this advisory it is possible to jeopardize critical telephony infrastructure based on Pingtel's xpressa SIP phones. Additionally, certain vulnerabilities present a severe risk to an organization's entire network infrastructure.

DETAILS

Securiteam: [NEWS] Multiple Vulnerabilities with Pingtel xpressa SIP Phones

Vulnerable systems:

- * Pingtel xpressa SIP VoIP phones model PX-1 versions 1.2.5–1.2.7.4

Remote Access Vulnerabilities

The Pingtel xpressa SIP-based phone provides a web interface that enables remote administrative configuration of the phone's settings. In addition, this web interface allows a remote user to place calls using SIP, install and remove applications, view and alter speed dial settings and configure call settings. Th