

[NEWS] Zyxel P2000W VoIP Wifi Phone Multiple Vulnerabilities

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2005-11/0082.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 11/21/05

To: list@securiteam.com

Date: 21 Nov 2005 17:06:17 +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>

Zyxel P2000W VoIP Wifi Phone Multiple Vulnerabilities

SUMMARY

" <<http://www.zyxel.com/product/P2000W.php>> ZyXEL's P-2000W VoIP Wi-Fi phone, compatible with IEEE 802.11b wireless standard, is a perfect solution for Voice over IP applications."

An undocumented open port and a static DNS record allow attackers to gain information, DoS and perform Man In the Middle attack against Zyxel's P2000W VoIP Wifi phone.

DETAILS

Vulnerable Systems:

* Zyxel P2000W version 1 firmware version Wj.00.10

Open Port:

The Zyxel P2000W VOIP WIFI phone has an undocumented port, UDP/9090, that provides an unauthenticated attacker information about the phone, specifically the phone's MAC address and software version is returned upon connection. An attacker can use this information for easily identify the phone and software version. Also, the undocumented open port provide an

Securiteam: [NEWS] Zyxel P2000W VoIP Wifi Phone Multiple Vulnerabilities

avenue for DoS.

Static DNS:

The Zyxel P2000W v.1 VOIP WIFI phone uses hard coded DNS servers located in Taiwan for the phone's DNS configuration.

Primary DNS IP is 168.95.1.1 resolving to dns.hinet.net
Secondary DNS IP is 139.175.55.244 resolving to dns.seed.net.tw

This configuration places every ZyXel phone using this software at risk of unintentional DoS if the DNS servers in Taiwan become unavailable. If the DNS servers are compromised, all Zyxel phone users worldwide are vulnerable to being redirected to malicious SIP servers, etc.

Workaround:

Users can manually input the IP address of a known, trusted DNS server via the keyboard at each phone start when configured for DHCP or PPOE, however, this will not persist once the phone is restarted.

ADDITIONAL INFORMATION

The information has been provided by <mailto:shawnmer@gmail.com> Shawn Merdinger.

=====

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.