

Cisco Security Notice: Response to BugTraq – The Trivial Cisco IP Phones Compromise

Document ID: 27150

Revision 1.0

For Public Release 2002 September 20

Please provide your feedback on this document.

Summary
Details
Cisco Security Procedures

Summary

This document is provided to simplify access to Cisco responses to possible product security vulnerability issues posted in public forums for Cisco customers. This does not imply that Cisco perceives each of these issues as an actual product security vulnerability. This notice is provided on an "as is" basis and does not imply any kind of guarantee or warranty. Your use of the information on the page or materials linked from this page are at your own risk. Cisco reserves the right to change or update this page without notice at any time."

Details

The original report can be found at: <http://www.securityfocus.com/archive/1/292460> . Cisco responded with the following which is also archived at <http://www.securityfocus.com/archive/1/292632/2004-08-14/2004-08-20/2> .

```
To: BugTraq
Subject: Re: The Trivial Cisco IP Phones Compromise
Date: Sep 19 2002 8:32PM
Author: Jim Duncan <jnduncan@cisco.com>
Message-ID: <200209192032.g8JKWhd11198@rooster.cisco.com>
In-Reply-To: <001d01c25fceb323e80$0a01a8c0@joshua>
```

-----BEGIN PGP SIGNED MESSAGE-----

Ofir Arkin writes:

```
> The referred paper lists several severe vulnerabilities with Cisco
> systems' SIP-based IP Phone 7960 and its supporting environment. These
> vulnerabilities lead to: complete control of a user's credentials; total
> subversion of a user's settings for the IP Telephony network, and the
> ability to subvert the entire IP Telephony environment. Malicious access
> to a user's credentials could enable "Call Hijacking", "Registration
> Hijacking", "Call Tracking", and other voice related attacks. The
> vulnerabilities exist with any deployment scenario, but this paper deals
> specifically with large scale deployments as recommended by Cisco.
```

```
>
```

```
> A PDF version of the paper is available from:
```

```
> http://www.sys-security.com/archive/papers/The\_Trivial\_Cisco\_IP\_Phones\_Compromise.pdf
```

This message contains Cisco responses to the issues described in the white paper referenced above.

1. Access to the Cisco 7960 IP phone:

A Cisco model 7960 IP phone running a SIP-compatible image has a password that can be set by the IP phone administrator. The default password is "cisco" if the password has not been set to some other value. Cisco strongly recommends setting the password to something other than the default.

The key sequence of "***#" is not intended as a password. It is clearly and publicly documented in many places within Cisco's product literature. The key sequence is solely intended to protect against casual or accidental changes to the phone's configuration.

2. Abuse of the TFTP service:

Although the author is correct that various attacks against the TFTP service can be mounted, there are several measures that can be employed by the IP phone administrator and the organization to mitigate the risk.

If the network is firewalled properly so that the different network segments are compartmentalized as the Cisco SAFE white papers recommend, then the TFTP server will only respond to legitimate requests. The TFTP server does not need to reside on the same network segment as the IP phone. If RFC 1918 addressing is employed for the IP phones and proper ingress/egress filtering is in place as recommended, then any such attack is highly unlikely to succeed from outside the enterprise VoIP network, even with the use of UDP. Access to the physical networks from within the enterprise may make it easier to succeed with the attack, but if the VLANs are properly protected and MAC addresses monitored per the SAFE documents -- for example, by using arpwatc or arpsnmp -- then an attack may be detected by the IP phone administrators.

3. Manual modification of the IP phone configuration:

At some level, successful attacks would require such physical access to the local network segment or the IP phone that the attacker could simply use the IP phone itself to commit toll fraud and some of the other improper acts listed in the paper. Physical access to network hardware is a long-standing, well-known problem in the industry. This is an especially important consideration for IP phones located in public or semi-public areas such as building lobbies. The IP phone administrator should use all available mechanisms to secure any IP phones that are exposed to unauthorized manipulation.

As always, Cisco is interested in protecting our customers' networks and is continually striving to improve the security of our products. We appreciate the seventeen days of advance notice we received from the author and his willingness to discuss the issue with us. We are unaware of any confirmed incidents of malicious exploitation of the issues in the author's paper and ask that any such exploitation be reported to the Cisco PSIRT, psirt cisco com, as soon as possible.

Cisco Security Procedures

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories

are available at <http://www.cisco.com/go/psirt>.

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Sep 20, 2002

Document ID: 27150
