

Cisco Security Response: Unconfirmed SIP Inspection Vulnerability

Document ID: 70977

<http://www.cisco.com/warp/public/707/cisco-sr-20060815-sip.sh>

Revision 1.0

For Public Release 2006 August 15 2000 UTC (GMT)

Please provide your feedback on this document.

[Cisco Response](#)
[Additional Information](#)
[Revision History](#)
[Cisco Security Procedures](#)

Cisco Response

This is the initial response from the Cisco Product Security Incident Response Team (PSIRT) in regards to a potential vulnerability originally disclosed at the recent Black Hat USA 2006 Briefings. In a presentation entitled "SIP Stack Fingerprinting and Stack Difference Attacks", Hendrik Scholz referenced a potential vulnerability in the way the Cisco PIX 500 Series Security Appliances handle inspection of Session Initiation Protocol (SIP) messages.

After extensive testing, Cisco has been unable to reproduce this issue and cannot confirm Mr. Scholz's claims.

Cisco will update this Security Response should new information become available.

Additional Information

The issue that Hendrik Scholz presented during his talk at the Black Hat USA 2006 Briefings relates to the way the PIX firewall handles the inspection of SIP messages. According to Mr. Scholz, upon receipt of a specially crafted SIP message, the PIX could open a User Datagram Protocol (UDP) connection to any device in the internal network. This connection would then allow an attacker to send UDP traffic to the internal device.

While Cisco was unaware of this potential vulnerability prior to the presentation, we have been working with Mr. Scholz to recreate the findings presented. To date, Cisco has not been able to create a vulnerable situation based on the description of the vulnerability as presented and on the information which he has further provided to Cisco. Consequently, no defect has been filed, although we will continue to work with Mr. Scholz as we attempt to recreate the situation and validate his claims.

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR

MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

Revision History

Revision 1.0	2006 August 15	Initial public release.
--------------	---------------------------	------------------------------------

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 © 1992–2006 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Aug 15, 2006

Document ID: 70977
