

# Cisco Security Response: Multiple SIP Vulnerabilities in the Cisco 7960 IP Phones

Document ID: 98592

<http://www.cisco.com/warp/public/707/cisco-sr-20070821-sip.shtml>

## Revision 1.1

Last updated 2007 August 22 1430 UTC (GMT)

For Public Release 2007 August 21 2200 UTC (GMT)

---

Please provide your [feedback](#) on this document.

---

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

---

## Cisco Response

This is the Cisco PSIRT response to an issue discovered and reported to Cisco by Radu State, Humberto J. Abdelnur and Olivier Festor regarding two Session Initiation Protocol (SIP) vulnerabilities in the Cisco 7940/7960 IP Phones.

The original reports are available at the following links:

<http://archives.neohapsis.com/archives/fulldisclosure/2007-08/0385.html>

<http://archives.neohapsis.com/archives/fulldisclosure/2007-08/0386.html>

We greatly appreciate the opportunity to work with researchers on security vulnerabilities, and welcome the opportunity to review and assist in product reports.

Cisco has confirmed the following: This issue is documented as Cisco bug ID [CSCsi68191](#) ([registered](#) customers only) . Cisco IP Phone 7940/7960 SIP firmware versions prior to 8.7(0) are vulnerable to the denial of service attacks detailed in the reports. Firmware versions 8.7(0) and later are not vulnerable to this issue. Version 8.7(0) firmware images for Cisco IP 7940/7960 phones can be obtained here:

<http://www.cisco.com/cgi-bin/tablebuild.pl/sip-ip-phone7960?psrtdcat20e2> ([registered](#) customers only)

## Additional Information

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 1.1	<del>2007–August–22</del>	<del>Corrected typo</del>
Revision 1.0	<del>2007–August–21</del>	<del>Initial public release</del>

## 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](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: Aug 22, 2007

Document ID: 98592

---