

Cisco Security Response: Cisco IOS Line Printer Daemon (LPD) Protocol Stack Overflow

Document ID: 99109

<http://www.cisco.com/warp/public/707/cisco-sr-20071010-lpd.shtml>

Revision 1.0

For Public Release 2007 October 10 1600 UTC (GMT)

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

[Cisco Response](#)

[Additional Information](#)

[Revision History](#)

[Cisco Security Procedures](#)

Cisco Response

This is the Cisco Product Security Incident Response Team (PSIRT) response to an issue discovered and reported to Cisco by Andy Davis from IRM, Plc. regarding a stack overflow in the Cisco IOS Line Printer Daemon (LPD) Protocol feature. The original post is available at the following link:

<http://www.irmplc.com/index.php/155-Advisory-024>

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

Additional Information

Cisco has confirmed the security research's findings and has documented this issue in Cisco Bug ID [CSCsj86725](#) ([registered](#) customers only).

All versions of IOS that support the LPD functionality except the ones listed below are affected. Customers that do not enable the LPD functionality are not affected.

Note: LPD is disabled by default on Cisco IOS routers.

If LPD services are configured, then one or more global **printer <name>** command lines would be present in the router's configuration.

No other Cisco products are currently known to be affected by this vulnerability.

This issue has been fixed on versions 12.2(18)SXF11, 12.4(16a), 12.4(2)T6 and later. For more information please view the bug's details via the Bug Toolkit on Cisco.com.

Workaround

If LPD services are not required, they can be disabled by using the **no printer** command; thus, eliminating this vulnerability.

Note: LPD is disabled by default on Cisco IOS routers.

In addition, LPD uses TCP port 515. An access control list (ACL) can be configured to only allow trusted devices to communicate to the router via TCP port 515.

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	2007–October–10	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 © 2006–2007 Cisco Systems, Inc. All rights reserved. [Important Notices](#) and [Privacy Statement](#).

Updated: Oct 10, 2007

Document ID: 99109
