

Cisco Security Response: HTTP Full-Width and Half-Width Unicode Encoding Evasion

Document ID: 91767

<http://www.cisco.com/warp/public/707/cisco-sr-20070514-unicode.shtml>

Revision 1.1

Last Updated 2007 May 18 1600 UTC

For Public Release 2007 May 14 2000 UTC (GMT)

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

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

Cisco Response

The U.S. Computer Emergency Response Team (US-CERT) has reported a network evasion technique using Unicode encoding that affects security products that perform deep packet inspection of HyperText Transfer Protocol (HTTP) requests. The US-CERT advisory is available at the following link:

<http://www.kb.cert.org/vuls/id/739224>

By encoding the Uniform Resource Locators (URLs) in HTTP requests using certain full-width or half-width Unicode characters, an attacker may be able to evade detection of the HTTP-based attack by an Intrusion Prevention System (IPS) or firewall. This may allow the attacker to covertly scan and attack systems normally protected by an IPS or firewall.

Cisco confirms that some Cisco products are affected by the vulnerability described in the US-CERT advisory.

This response is posted at the following link:

<http://www.cisco.com/warp/public/707/cisco-sr-20070514-unicode.shtml>

Additional Information

Security devices perform deep packet inspection of HTTP traffic to try to detect and stop HTTP-based attacks. Examples of security devices that perform this function include IPS and firewalls.

For these devices to be able to perform this function correctly they need to be able to understand how the URLs in HTTP requests are encoded. Hexadecimal and Unicode encoding are examples of URL encoding methods.

Vulnerability Note VU#739224 from the US–CERT reports that it is possible to hide HTTP–based attacks by encoding URLs using half–width or full–width Unicode characters. This is possible because devices performing deep packet inspection of HTTP traffic may fail to properly decode URLs encoded using this method, and therefore, fail to recognize potentially harmful URLs. The affected Cisco security products are able to decode full–width and half–width Unicode characters, however certain characters are not decoded properly.

The following Cisco products are affected by this vulnerability (all versions are affected unless a specific version is explicitly mentioned):

- Cisco Intrusion Prevention System (IPS).

This issue is documented for Cisco IPS sensors in Cisco Bug ID [CSCsi58602](#) ([registered](#) customers only)

- Cisco IOS with Firewall/IPS Feature Set.

IOS devices are affected when the Context–Based Access Control (CBAC, also known as IOS Firewall) or IPS functionality is enabled.

CBAC is enabled and performing deep packet inspection of HTTP traffic when the global configuration command **ip inspect name <NAME> http** and the interface configuration command **ip inspect <NAME> in/out** are present.

IOS IPS is enabled when the statement **ip ips <NAME> in/out** is present under interface configuration mode.

This issue is documented for Cisco IOS in Cisco Bug ID [CSCsi67763](#) ([registered](#) customers only) .

- Cisco Adaptive Security Appliance (ASA) and PIX Security Appliances.

PIX and ASA Security Appliances are affected when inspection of HTTP traffic is enabled via the command **inspect http**.

Only PIX and ASA software versions 7.x and later are affected; PIX software versions 6.x and before are not affected.

This issue is documented for Cisco PIX/ASA Security Appliances in Cisco Bug ID [CSCsi91487](#) ([registered](#) customers only) .

None of the products referenced in this Security Response can be compromised by a HTTP–based attack hidden by the Unicode encoding technique; these products might fail to recognize a HTTP–based attack against the infrastructure that they are monitoring or protecting.

Currently there are no software fixes available to address this vulnerability, however, once there are, we will make them available to affected customers.

The Cisco PSIRT is not aware of any malicious use of the vulnerability described in this document.

This issue was reported to Cisco by US–CERT. The original issue was reported to US–CERT by Fatih Ozavci and Caglar Cakici of Gamasec Security. Cisco would like to thank US–CERT, Fatih Ozavci and Caglar Cakici for bringing this issue to our attention.

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	2007–May–18	Added the PIX and ASA products to the list of affected products. Minor wording changes.
Revision 1.0	2007–May–14	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: May 18, 2007

Document ID: 91767
