

Vulnerability Advisory

Name	TippingPoint IPS Signature Evasion
Vendor Website	http://www.Tippingpoint.com
Date Released	July 11 th , 2007
Affected Software	TippingPoint IPS running TOS versions 2.1, 2.2.0 - 2.2.4, 2.5.0 - 2.5.1 (versions prior to 2.2.5 and 2.5.2)
Researcher	Paul Craig : paul.craig@security-assessment.com

Description

During security analysis of the Tippingpoint IPS product a signature evasion vulnerability was discovered. The use of specific Unicode characters on particular web servers allows a remote user to bypass IPS detection.

Exploitation

By using a hex encoded alternate Unicode character for forward slash (/) a request can be produced that will not match any IPS signature present in the TippingPoint device.

Example:

<http://www.test.com/scripts/cmd.exe> is a known attack and detected by a signature.

The same URI with alternate Unicode forward slash characters are not detected by the signature.

<http://www.test.com/scripts%c0%afcmd.exe>
<http://www.test.com/scripts%e0%80%afcmd.exe>
<http://www.test.com/scripts%c1%9ccmd.exe>

Web servers located behind a Tippingpoint IPS device which are capable of decoding alternate Unicode characters can be accessed, and exploited without triggering the IPS device.

Solution

- Security-Assessment.com has been in contact with Tipping and a new version of the Tippingpoint IPS software has been released to address the discovered vulnerability. This issue has been addressed in various TOS releases as indicated by the affected product below.
 - X-Family devices, 2.5.0.6682.
 - non-X-Family device (not including 600E, 1200E, 2400E or 5000E), 2.5.1.6826.
 - non-X-Family device (including 600E, 1200E, 2400E or 5000E), 2.5.2.6919.

About Security-Assessment.com

Security-Assessment.com is a leader in intrusion testing and security code review, and leads the world with SA-ISO, online ISO17799 compliance management solution. Security-Assessment.com is committed to security research and development, and its team have previously identified a number of vulnerabilities in public and private software vendors products.

For further information on this issue or any of our service offerings, contact us

Web www.security-assessment.com
Email info@security-assessment.com
Phone +649 302 5093