CYBSEC S.A.
www.cybsec.com

Advisory Name: TippingPoint detection bypass

Vulnerability Class: Design flaw

Release Date: 2007-07-04

Affected Platforms:
- TippingPoint IPS running TOS versions 2.1.x, 2.2.x prior to 2.2.5, and 2.5.x prior to 2.5.2

Local / Remote: Remote

Severity: High

Author: Andrés Riancho

Vendor Status:
- Confirmed. Updates Released.

Reference to Vulnerability Disclosure Policy:
http://www.cybsec.com/vulnerability_policy.pdf

Product Overview:

"The TippingPoint Intrusion Prevention System (IPS) is an award-winning security solution that blocks worms, viruses, Trojans, Denial of Service and Distributed Denial of Service attacks, Spyware, VoIP threats, and Peer-to-Peer threats. Inspecting traffic through Layer 7, the IPS blocks malicious traffic before damage occurs."

Vulnerability Description:

When IP packets are fragmented in a special way, the appliance fails to correctly reassemble the data stream.

Technical Details:

Technical details will be disclosed 30 days after publication of this pre-advisory. This was agreed upon with TippingPoint to allow their customers to upgrade affected software prior to technical knowledge been publicly available.

Impact:

Exploiting this vulnerability, an attacker would be able to bypass all filters and detection.

Solutions:

TippingPoint has released a new version of the TippingPoint OS to address this vulnerability. Customers should apply the new firmware immediately. More information can be found at http://www.3com.com/securityalert/alerts/3COM-07-002.html

Vendor Response:

- 2006-02-06: Initial Vendor Contact.
- 2006-06-20: Vendor Confirmed Vulnerability.
- 2007-07-04: Vendor Releases Update.

Contact Information:

For further information regarding the vulnerability feel free to contact the author at ariancho {at} cybsec.com.

For more information regarding CYBSEC: www.cybsec.com (c) 2007 - CYBSEC S.A. Security Systems