



CYBSEC S.A.

www.cybsec.com

Pre-Advisory Name: 3com - TippingPoint IPS Detection Bypass

Vulnerability Class: Design Flaw

Release Date: 07/24/2006

Affected Platforms:

- All TippingPoint Appliances with TOS ≤ 2.2.3.6514

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) delivers the most powerful network protection in the world. The TippingPoint IPS is an in-line device that is inserted seamlessly and transparently into the network. As packets pass through the IPS, they are fully inspected to determine whether they are legitimate or malicious.”

Vulnerability Description:

A malformed packet can force the appliance to fallback to layer 2 mode. In this mode the appliance forwards all traffic without inspection.

Technical Details:

Technical details will be released 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.

Vendor Response:

- 06/02/2005: Initial Vendor Contact.
- 06/20/2006: Vendor Confirmed Vulnerability.
- 07/21/2006: Vendor Releases Update.
- 07/24/2006: Pre-Advisory Public Disclosure.

Contact Information:

For more information regarding the vulnerability feel free to contact the author at ariancho [at] cybsec.com. Please bear in mind that technical details will be disclosed to the general public three months after the release of this pre-advisory.

For more information regarding CYBSEC: www.cybsec.com