Security Advisory for Bash "Shellshock" Vulnerabilities

Revised 10/14/14

Ixia is notifying you regarding the recent vulnerability in the Bourne Shell (aka Bash). Recently, a vulnerability was disclosed that could put some systems running Bash at risk for remote exploitation. The vulnerability could allow a local or remote attacker to utilize specially crafted input to execute arbitrary commands or code. Due to the risk that this may present, it is advised that any vulnerable systems have a patch applied to remediate the vulnerability. The vulnerability is identified with multiple CVE identifiers.

- CVE-2014-7169, CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7186, CVE-2014-7187
-

Ixia has determined that the products listed below are susceptible and should be updated as soon as possible to remediate the vulnerability. Updates that include the patch will be available from Ixia support.

- Indigo Pro
- xFilter
- Spyke
- BPS Storm (Dec 2014)
- BPS FireStorm(Dec 2014)
- PerfectStorm (Dec 2014)
- PerfectStorm ONE (Dec 2014)
- IxVM (Dec 2014)
- IxCatapult P250, X100 DCT, X100 & X800 (1Q15)

Ixia has determined that the products listed below are not susceptible to the Bash vulnerability and require no update at this time.

- NTO 5204, 5236/5273, 5288/5293, 5260, 5263/5268, 2112/2113, 7433, 7300/7303, 6212
- Phantom vTap
- TradeView 1000
- xStream 10/40
- Director
- iLinkAgg
- All Taps and Bypass Switches
- IxLoad (Non-PerfectStorm Fusions)

- IxNetwork
- IxVeriwave
- Ixia Anue Network Emulators
- Ixia Anue 3500
- NGTS
- IxN2X
- IxANVL

The Ixia products listed below include an affected version of the Bash executable in some form but are not susceptible to exploitation of the vulnerability and will be patched in their next scheduled release.

- NTO 7300/7303 v4.0.5 (Dec 2014)
- Phantom vTap v3.5.0 (Oct 2014)
- xStream 10/40 v6.5.0 (Nov 2014
- Director v7.9.0 (Oct 2014)
- iBypassHD v3.0.0 (Nov 2014)

If you have questions regarding an Ixia product's susceptibility to the Bash vulnerability or the updates required to remediate the vulnerability, please contact Ixia support at http://www.ixiacom.com/support-services/contact-support.