Security Advisory

# Security Advisory for POODLE Vulnerabilities

**Revised 03/2015**

Ixia has confirmed that the SSL v3 POODLE vulnerability impacts some of its visibility products. Comprehensive fixes to be released per the schedule below.

In order to exploit the vulnerability, a malicious user must have access to a device which can intercept the client/server SSL connection. Deploying equipment behind a firewall dilutes the risk.

**Products and Releases not Vulnerable**

| | |
|---|---|
| NTO 5204, 5236, 5273, 5288, 5293 (NVOS 3.x) | 3.10 or later |
| NTO 730x (NVOS 4.0.x) | 4.0.5 or later |
| GSC 7433 | 1.4.0 or later |
| iBypassHD | 4.1.4 or later |
| Phantom | 3.5 patch or later |

**Affected Products with future patch releases**

| | |
|---|---|
| NTO 5260, 5268, 5263, 5288, 5293 (NVOS 4.x) | Fix release available April 2015 |
| xStream | Fix available April 2015 |
| iLinkAgg/iPA2/iBypass2/iBypass3 | Fix release to be scheduled |
| Spyke | Fix release to be scheduled |

As a general security precaution, Ixia suggests disabling SSLv3 on all client machines and ensure that TLS encryption is enabled.