ION Networks
120 Corporate Boulevard, South Plainfield, NJ 07080
Tel: +1 908/546/3900 Fax: +1 908/546/3901
www.apitech.com/ION

Revised November 17, 2014

ION Networks Products and the 'Shellshock' BASH Vulnerability

A significant information security vulnerability with the BASH Shell was recently identified. This shell is present in most Linux and Unix operating systems deployed today. This vulnerability was initially tracked as CVE-2014-6271 and has commonly become known as "Shellshock". ION Networks products, like many others that incorporate a BASH are affected by this vulnerability to varying degrees.

The current evaluation of this vulnerability with regards to ION security products is detailed below. To ensure the security of your networks and devices remains uninterrupted, our engineering team has created upgrades for customers with SecureCare. For customers without maintenance we have created security patches for some appliances versions (1.2.3 up).

To request a patch, send an email to: ion.networks.support@apitech.com. Please include the name of the product in your request.

ION Networks products *not vulnerable* to the Shellshock flaw:

Product Family	Version
SM110	All
PRIISMS	All
ST520	All
ST530	All
ION Secure 3500*	All
ION Secure 5500*	All

Product Family	Version
Netgard MFD	All
ASG Guard*	All
ASG Guard II*	All
ASG Guard Plus*	All

* End of Life

ION Networks products affected by the Shellshock vulnerability:

Product Family	SW Version	BASH Version Vulnerable	BASH exploitable remotely	Resolution
Defender	All	Yes	No	Upgrade to version 1.0.6[#], then patch with Shellshock4.BIN
SA500	All	Yes	No	Patch with Shellshock4.BIN or upgrade to APP-1.3.0-B91.BIN
SA600	All	Yes	No	Patch with Shellshock4.BIN or upgrade to APP-1.3.0-B91.BIN
SA5600	All	Yes	No	Patch with Shellshock4.BIN or upgrade to APP-1.3.0-B91.BIN

ION Networks
120 Corporate Boulevard, South Plainfield, NJ 07080
Tel: +1 908/546/3900 Fax: +1 908/546/3901
www.apitech.com/ION

Product Family	SW Version	BASH Version Vulnerable	BASH exploitable remotely	Resolution
PR-RD-DT (aka the RD)	All	Yes	No	Patch with Shellshock4.BIN or upgrade to ROUTER-1.3.0-B45.BIN
SA5600-DEF	All	Yes	No	Patch with Shellshock4.BIN
SA5600-SAL	All	Yes	Yes	Install ION.SEC.4.TGZ. **Caution do not use Shellshock4.BIN**
SA5600-IA2	All	Yes	No	Install APP-1.3.1-B28.BIN
PR-RD-DT-IA2 (aka the RD)	All	Yes	No	Install ROUTER-1.3.1-B23.BIN

[#]For a limited number of Defenders, an additional step must be taken to install shellshock4.bin. Please contact ION Network Support if after application of the patch, the ver full command does not list the patch as applied.

Note that the remote vulnerability exposed in general purpose installations of Linux does not apply to the ION builds of appliances (except –SAL versions) as the remote attack vectors are not available on these platforms. This should be considered in your evaluation of risks. The vulnerability affected the ION products in the use of the open source tool BASH. Ion appliances do not contain Apache, nor vulnerable DHCP clients. BASH is used for general purpose shell scripting and is only available to authorized users.

The vulnerabilities CVE-2014-6271, CVE-2014-6277, CVE-2014-6278, CVE-2014-7169, CVE-2014-7186, and CVE-2014-7187 are all addressed by the patches and upgrades listed above. A patched appliance will show “Shellshock patch2” within the response to the “ver all” command to indicate that the patch has been applied.

If you have any further questions or concerns, please contact ION Networks Technical Support at +1 908-546-3900 Option 2 or by emailing ion.networks.support@apitech.com.

Thank you,

Peter Paulson
Director of Engineering and Operations