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

September 30, 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 CVE-2014-7169. It 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 is creating security patches.

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
Netgard MFD	All

ION Networks products affected by the Shellshock vulnerability:

Product Family	**SW Version**	**BASH Version Vulnerable**	**BASH exploitable remotely**	**Resolution**
SA500	All	Yes	No	Patch with Shellshock.BIN or upgrade to APP-1.3.0-B91.BIN
SA600	All	Yes	No	Patch with Shellshock.BIN or upgrade to APP-1.3.0-B91.BIN
SA5600	All	Yes	No	Patch with Shellshock.BIN or upgrade to APP-1.3.0-B91.BIN
Defender	All	Yes	No	Patch with Shellshock.BIN
PR-RD-DT (aka the RD)	All	Yes	No	Patch with Shellshock.BIN or upgrade to ROUTER-1.3.0-B45.BIN
SA5600-SAL	All	Yes	Yes	Install ION.SEC.4.TGZ

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
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

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.

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