OCT 2014

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the October 2014 edition of In the Boxing Ring

This month, we talk in detail about **CVE-2014-6271** and **CVE-2014-7169** bash vulnerabilities or commonly named, **Shellshock**. The vulnerability proved to be extremely exploitable, and both security researchers and malicious agents started to mass scan the entire Internet looking for vulnerable servers. This is is discussed further on pages 2-3.

On pages 4-5, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5 and Network Box 3. We continue to develop, and will continue to support, Network Box 3 for the foreseeable future (several years).

Finally, Network Box is conducting a number of seminars about Advanced Persistent Threats (APTs). These are targeted attacks specifically designed to infiltrate your network and steal your data. The real danger of APTs, and what makes them unique, is that they remain in your network for a long period of time, moving 'low and slow', making them hard to detect. In addition, Network Box was covered in IT-Security Guide and Australian Security Magazine.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
October 2014

You can contact us here at HQ by eMail (nbhq@network-box.com), or drop by our office next time you are in town. You can also keep in touch with us by several social networks:

twitter http://twitter.com/networkbox

facebook http://www.facebook.com/networkbox
http://www.facebook.com/networkboxresponse

LinkedIn http://www.linkedin.com/company/network-box-corporation-limited

Google+ https://plus.google.com/u/0/107446804085109324633/posts

In this month's issue:

NETWORK BOX

On the 25th September a vulnerability in the bash shell, commonly used with Unix/Linux products, was announced and given the identifier CVE-2014-6271. The vulnerability proved to be extremely exploitable, and both security researchers and malicious agents started to mass scan the entire Internet looking for vulnerable servers.

Almost immediately upon the public release of patches, security researches started to question the effectiveness and completeness of the official fixes. Sure enough, a subsequent vulnerability (CVE-2014-7169) was announced, documenting a new way of exploiting even patched systems.

Network Box Security Response announced Threat Level 4 (to put that into perspective, we had not been at that level, for this serious a vulnerability, since 2006), and a lot of sleep was lost providing patches and protection signatures against all the scanning and exploit activity. The popular name 'shell shock' was given to describe this new threat - and it was an apt name, given how many in the security industry felt after the first 24 to 48 hours of dealing with the fallout from this new threat.

What is Bash Shellshock?

So, what is *bash* Shellshock, and the CVE-2014-6271 and CVE-2014-7169 vulnerabilities?

Simply put, the *bash* shell has a facility whereby functions (executable commands) can be put into environment variables, and when a new bash shell is executed with that environment, it executes those commands. The vulnerability is that if an attacker can control what goes into environment variables, and if the vulnerable program executes the bash shell, then the commands will run (with the security credentials of the program executing bash). This is a classic remote-exploit.

A simple example to show the vulnerability at the command line is:

```
env x='() { :;}; echo I am
vulnerable' bash
```

That sets the environment variable *x* to the value *'() { :;}; echo I am vulnerable'*, and then executes the *bash* shell. The result is that "I am vulnerable" is printed on the console.

> Note that the vulnerability is actually more accurately described as that the executable commands can be put after the function definition, but from the attacked system's point of view it makes little difference

The reason that the issue is so serious is because it turns out that it is not difficult to get arbitrary data into environment variables. For example, the popular CGI scripting system (used by an enormous number of public-facing web servers) will put the headers provided to the web server into environment variables, prior to executing the CGI script. Exploit is as simple as setting the user agent in the web request to be the exploit code. The only thing stopping exploit is then whether the CGI script actually executes the *bash* shell.

Some DHCP clients also appear to be similarly vulnerable (they put options provided by the DHCP server into environment variables, prior to executing *bash* to configure the network interface), and more and more possible exploit vectors are being found each day.

Current Situation

The current situation for Network Box customers is that we have released (and continue to release) NBIDPS and WAF+ signatures to protect against exploit. We continue to see extensive scanning activity (both malicious and reconnaissance), although this has died down in recent days.

However, it must be pointed out that gateway-level protection is only one part of a defence-in-depth strategy. While we can protect against know exploits, vulnerabilities such as this have proven in the past to be exploitable in new and inventive ways - and sometimes those exploits come from within the network (not even passing through the gateway). The DHCP vector is particularly concerning.

Now that full comprehensive patches have been released by the vendors, and those patches address both CVE-2014-6271 and CVE-2014-7169 vulnerabilities, Network Box Security Response has been working with local NOCs and customers to actively patch potentially vulnerable servers. We continue to recommend and strongly encourage customers to conduct an internal audit to enumerate potentially vulnerable systems, and to ensure that those systems are patched.

Given the state of our signature protection, and patch levels of our customer base, Network Box Security Response last night lowered our alert level to 3, and will consider further lowering it in the coming days.

The Future

The biggest concern with these vulnerabilities is that they will be exploitable by a network worm. Should a large number of vulnerable systems remain un-patched, and a mass exploitable vector be discovered, that remains a very real possibility. The only way to comprehensively protect against this is by ensuring potentially affected systems are patched. There are a very large number of embedded and other such devices running Linux.

For our customers, Network Box Security Response continues to closely monitor the situation and refine our signature protection to address new and emerging variants of these exploits.

NETWORK BOX

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 7th October 2014, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days.

Network Box 5 Features
October 2014

This month, for Network Box 5, these include:

- CVE-2014-6271: bash environment variables code injection attack (support released out-of-cycle 2014-09-25)
- CVE-2014-7169: Shellshock2 (support released out-of-cycle 2014-09-26)
- New feature to provide ability to choose source IP with ping and traceroute commands
- Enhanced geo-location database for improved accuracy and coverage
- Revisions to default values for kernel watchdog timers
- Enhancement to provide support for UTF-8 character sets in console output
- Introduction of a facility to support the suppression of GMS sensors
- Performance and stability improvements to logging facility
- Performance and stability improvements to quarantine container facility
- Change to default values for GMS memory sensor, to relax swap space criteria
- Support for keeping network interfaces disabled on boot (used for high-availability configurations)
- Enhanced support for High Availability bridge configurations
- Enhanced support for pure-virtual High Availability configurations (without virtual IP addresses)
- Improvements to configuration search facility
- Introduction of case insensitivity, during authentication
- Improvements to multi-link gateway handling, and link failure recovery
- Introduction of an administrative watchdog reboot facility
- Improved support for multiple ADSL links
- Improved monitoring and control of ADSL links
- Introduction of a GMS sensor for ADSL/PPPoE links
- Inclusion of Firewall, IDS, and IPS KPIs in default report
- Improvements to Kaspersky anti-malware engine, with configurable heuristic level and faster signature reload
- Support for nBus communication protocol (in provisioned cluster sync connections)
- Various improvements to SNI categorisation (for policy control of SSL connections based on client SNI option)
- Enhanced support in mail scanning for URL analysis, by public suffix list (PSL)
- Performance improvements in mail scanning policy enforcement (via rules engine)
- Introduction of a 'releaseall' option to quarantine release (to release to all recipients)
- Performance and stability improvements to Admin and User Portal web interfaces
- Enhancement to show the threat (for malware blocks) in user portal report
- Change to user portal report to not count failed deliveries in the summary totals
- Enhancement to admin portal web interface to add support for HTTPHOST ACLs
- Introduction of a new KPI for MEMORY utilisation
- Introduction of a new KPI for WAF
- Introduction of a new optional facility to enforce Safe Search at the proxy, for Google, Yahoo and Bing
- Performance and compatibility improvements in the proxy facilities (for HTTP, POP3 and SMTP protocols)
- Improved support for SMTP AUTH in Outlook
- Introduction of TCP and UDP congestion control, to reduce memory requirements of proxy during large file transfers
- Kernel upgrade to improve performance and compatibility at the network driver level

Due to the kernel upgrade in this month's release, a device restart will be required. Local SOCs will be arranging this with you, if necessary, according to standard arrangements.

Should you need any further information on any of the above, please contact your local SOC. They will be arranging deployment and liaison.

NETWORK BOX

Network Box ISO 9001 / ISO 20000 / ISO 27001 certified Security Operations Centre, ensures that customers' networks are protected against cyber threats, 24x7x365.

Network Box 3 Features October 2014

On Tuesday, 7th October 2014, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, for Network Box 3, these include:

- Improvements to spam detection, related to exploits against new top level domains
- Improvements to my.network-box.com facility for restarting a failed SSL VPN link
- CVE-2014-6271: bash environment variables code injection attack (released out-of-cycle 2014-09-25)
- CVE-2014-7169: Shellshock2 (released out-of-cycle 2014-09-26)
- Various (mostly internal) enhancements to several internal support systems

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local SOC will contact you to arrange this if necessary.

Network Box Germany
IT-Security Guide

Network Box Germany was featured in the latest IT-Security Guide. As well as highlighting Network Box, the 'Vulnerability of Everything,' is also discussed in the double page article.

LINK:
http://www.isreport.de/epaper/Files%20Sec/

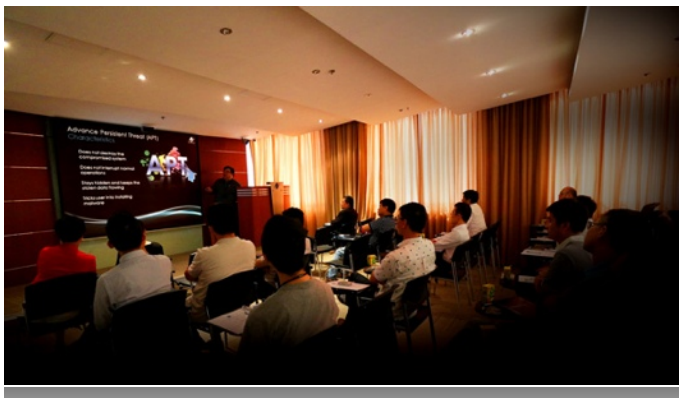
Australia Security Magazine
How to be a Prepper

Network Box's CTO, Mark Webb-Johnson, was featured in 'Australian Security Magazine,' talking about how to defend networks against Distributed Denial of Service (DDoS) attacks.

LINK:
https://www.australiansecuritymagazine.com.au/2014/08/prepper-aka-survive-ddos-attack/

Network Box Security Seminar
Advanced Persistent Threats (APTs)

Network Box is holding a number of seminars about Advanced Persistent Threats (APT), which are a type of targeted attack, that use a wide variety of techniques to infiltrate your network, and steal your data. The real danger, and what makes APT unique, is that it moves 'low and slow' within your network, allowing it to stay under the radar, remaining hidden and hard to detect. The goal is long term gain, as opposed to the usual 'smash and grab' form of cyber attack.



Newsletter Staff	Subscription
Mark Webb-Johnson Editor **Michael Gazeley** **Nick Jones** **Kevin Hla** Production Support **Network Box HQ** **Network Box UK** **Network Box USA** Contributors	Network Box Corporation nbhq@network-box.com or via mail at: **Network Box Corporation** 16th Floor, Metro Loft, 38 Kwai Hei Street, Kwai Chung, Hong Kong Tel: +852 2736-2078 Fax: +852 2736-2778 www.network-box.com

Copyright © 2014 Network Box Corporation Ltd.