FEB 2015

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the February 2015 edition of In the Boxing Ring

In light of the bash shellshock vulnerability, heartbleed, and more recently, the glibc ghost vulnerability; this month, we talk about **Core Library Vulnerabilities**. In the past year, we've seen a number of core library level vulnerabilities affecting multiple applications in multiple different ways. This is a worrying trend where the application itself is not targeted, but instead one of the system core libraries it uses has a vulnerability that can be exploited through the application. This is discussed further on page 2.

On pages 3–4, 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 proud to announce that we are the only Managed Security Service Provider to be named as a finalist of the SC Magazine 2015 Excellence Awards. Winner will be honored in San Francisco, on 21 April 2015.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
February 2015

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

Core Library Vulnerabilities

For many years now, we've become accustomed to seeing application vulnerabilities, with some of these being remotely exploitable and the worst being in network services. We've learnt how to categorize and prioritize these threats, and have good response procedures in place to mitigate and respond to them.

However, in the past year, we've seen a number of core library level vulnerabilities affecting multiple applications in multiple different ways. This is a worrying trend where the application itself is not targeted, but instead one of the system core libraries it uses has a vulnerability that can be exploited through the application. Such exploits are often remotely achievable.

Examples of this include the **bash shellshock** vulnerability, **heartbleed** and other issues in the core openssl library, and most recently the **glibc ghost** vulnerability.

In the face of these new types of vulnerabilities, as an industry, we've got to learn new techniques to handle them from a security response point of view.

Some things to bear in mind include:

- In the case of application vulnerabilities, there is usually only one exploit vector. But, in the case of core library vulnerabilities, each application that uses that core library may have many possible exploit vectors.
- Detecting core library exploit code, at the network level, with so many possible exploit vectors, is not at all straightforward (especially compared to application vulnerabilities). A single core library exploit may require dozens of signatures to cover even just the common exploit vectors.
- Once an application is patched to address a particular vulnerability, the application can simply be restarted to install the fix (which is commonly even part of the automatic patch application script). However, for core library vulnerabilities, after applying the patch you must manually identify and restart each affected service.
- Services using the Unix/Linux fork-and-exec approach won't automatically pick up a newly patched core library and will continue to fork copies of vulnerable code until restarted.
- The safest approach is a complete system reboot, but that can be obtrusive and impact service delivery.

Network Box Security Response, as are others in our industry, are working hard to introduce security technologies and revise our response procedures to address these and other such vulnerabilities. In the case of known core library exploits that could affect the Network Box itself, we'll remotely patch and restart affected services. In the case of vulnerabilities that affect protected customer systems, we work with our industry partners to identify possible exploit vectors and address those appropriately.

NETWORK BOX

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 3rd February 2015, 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
February 2015

This month, for Network Box 5, these include:

- Improvements to CSV export facility, in cases where report contains a large number of records
- Update to the latest version of Kasperky anti-malware scanning engine
- Enhancement to sum up confidence levels even for clean email
- Enhanced support for SMTP AUTH for delivery of reports and alerts from the box
- Additional support for specification of webclient output sourceip, when in directed proxy mode
- Support IP type ACLs in routing statements
- Improvements to administrator notification for GMS and other alerts
- Improvements to logging, after ssl decode bypass
- Support for tab-expansion in urlhostpathwildcard for proxy webclient policy rules
- Improvements to 'config search' facility for administrators
- Additional support for new report time range options in user portal
- Introduction of Mail Server security module (for on-the-box mail queueing and routing)
- Provide an option to remove the whitelist option on user portal web and report
- Enhanced policy control for SSL in network outbound policy
- Enhanced policy control for IPv4/IPv6 selection in network outbound policy
- Fix to GMS reporting, in situations where network connectivity is intermittently faulty
- Provide a better filename suggestion when exporting SSL CA certificate
- Improvements to logging of webclient www.http and www.https connections
- Permit fine-grained control of scan result confidences less than 100%
- German translation for admin and user portal
- CVE-2014-3511: The ssl23_get_client_hello function in s23_srvr.c in OpenSSL
- CVE-2014-3512: Multiple buffer overflows in crypto/srp/srp_lib.c in SRP in OpenSSL
- CVE-2014-3510: The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL
- CVE-2014-3507: Memory leak in d1_both.c in the DTLS implementation in OpenSSL
- CVE-2014-3506: d1_both.c in the DTLS implementation in OpenSSL
- CVE-2014-3505: Double free vulnerability in d1_both.c in the DTLS implementation in OpenSSL
- CVE-2014-3509: Race condition in the ssl_parse_serverhello_tlsext function in t1_lib.c in OpenSSL
- CVE-2014-5139: The ssl_set_client_disabled function in t1_lib.c in OpenSSL
- CVE-2014-3508: The OBJ_obj2txt function in crypto/objects/obj_dat.c in OpenSSL
- CVE-2014-3568: OpenSSL 1.0.1 does not properly enforce the no-ssl3 build option
- CVE-2014-3567: Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL
- CVE-2014-3513: Memory leak in d1_srtp.c in the DTLS SRTP extension in OpenSSL
- CVE-2014-3569: The ssl23_get_client_hello function in s23_srvr.c in OpenSSL
- CVE-2014-8275: OpenSSL 1.0.1 does not enforce certain constraints on certificate data
- CVE-2014-3572: OpenSSL 1.0.1 allows remote SSL servers to conduct ECDHE-to-ECDH downgrade attacks
- CVE-2015-0204: OpenSSL 1.0.1 allows remote SSL servers to conduct RSA-to-EXPORT_RSA downgrade attacks
- CVE-2014-3570: The BN_sqr implementation in OpenSSL 1.0.1 does not properly calculate the square of a BIGNUM value
- CVE-2015-0205: OpenSSL 1.0.1 accepts authentication with DH certificate without CertificateVerify
- CVE-2015-0206: Memory leak in the dtls1_buffer_record function in d1_pkt.c in OpenSSL
- CVE-2014-3571: OpenSSL 1.0.1 DTLS message read operation Denial of Service
- CVE-2015-0235: __nss_hostname_digits_dots heap buffer overflow
- CVE-2014-0475: directory traversal via a .. in LC_* and LANG env variables
- CVE-2014-5119: Crash due to off-by-one error in the __gconv_translit_find
- CVE-2013-4237: Buffer overwrite when using readdir_r
- CVE-2013-4458: Stack-based buffer overflow in the getaddrinfo function
- CVE-2014-6040: Out-of-bounds read and crash in the iconv function
- CVE-2014-7817: Wordexp function does not enforce the WRDE_NOCMD flag
- Migration to nBus, for configuration synchronisation
- Migration to nBus, for initial box provisioning
- Migration to nBus, for signature push
- 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.

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 February 2015

On Tuesday, 3rd February 2015, 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:

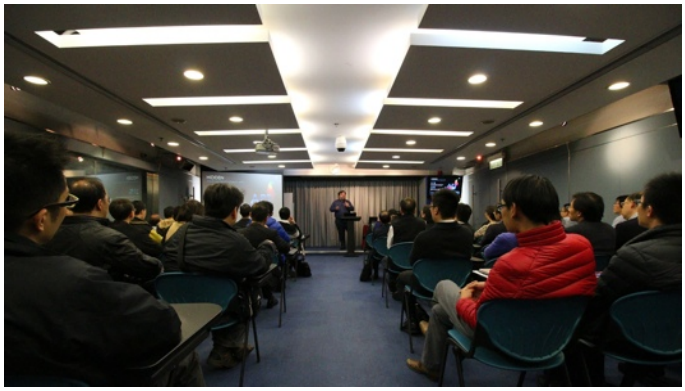
- CVE-2015-0235: __nss_hostname_digits_dots heap buffer overflow
- Various (mostly internal) enhancements to several internal support systems

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.

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 2736-2083 Fax: +852 2736-2778 www.network-box.com

Network Box Hong Kong
ISACA CPD Seminar

Network Box Managing Director, Michael Gazeley, gave a seminar outlining the current Cyber Risk Landscape 2015, and the increasing 'Vulnerability of Everything.' As more and more smart connected devices are being installed in homes and offices, such as printers, fax machines, telephones, televisions, video surveillance, webcams, copiers, etc, they are fast making us all more and more vulnerable to cyber criminals and hackers.



Network Box
SC MAgazine Awards 2015

Network Box was named SC Magazine 2015 Excellence Award Finalist in the category of Best SME Security Solution. Network Box is the only Managed Security Service Provider to make it into the finals.

LINK: http://www.scmagazine.com/2015-sc-awards-us-finalists-round-one/article/392347/

Network Box HQ
Network Box 5 Training and Seminars

Network Box China, and **Network Box Taiwan**, were both at Network Box HQ, for technical training with Mark Webb-Johnson, Network Box's CTO, on the very latest Network Box 5 features.