In the Boxing Ring
SEP 2023

Network Box Technical News
from Mark Webb-Johnson
Chief Technology Officer, Network Box

Welcome to the September 2023 edition of In the **Boxing Ring**

This month, we are talking about the **Barracuda ESG Zero-Day Vulnerability**. Earlier in 2023, Barracuda Networks discovered unusual traffic from some of their ESG (Email Security Gateway) appliances. They followed this up with public disclosure of the issue labelled *CVE-2023-2868* - a remote command injection vulnerability with evidence of in-the-wild exploitation. Later, however, Barracuda shocked the security industry with an update saying that all impacted devices should be completely replaced (not just patched), irrespective of firmware or patch level. Such a global recall was unprecedented and indicated a problem far more severe and deeply embedded than first thought. On pages 2 to 3, we go through the timeline of events and discuss the vulnerability in greater detail.

On page 4, we highlight the set of enhancements and fixes to be released in this month's Patch Tuesday for Network Box 5 and our cloud services.

In other news, Network Box is pleased to announce a partnership agreement with **Larix Industries** to offer our security solutions to customers in Mongolia and Kazakhstan. Additionally, Network Box participated in the **SmartLife Technology Forum**, which took place at the National University of Mongolia. And in this month's global security headlines, there were security issues with **Cisco** VPNs, **Juniper** Firewalls, and **Barracuda** ESG appliances.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
September 2023

Stay Connected

You can contact us here at Network Box 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:

https://twitter.com/networkbox

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

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

https://www.youtube.com/user/NetworkBox

In this month's issue:

BARRACUDA ESG Zero-Day Vulnerability

In mid-May 2023, Barracuda (a manufacturer of network security appliances) discovered unusual traffic coming from some of their ESG (Email Security Gateway) appliances. These appliances filter email for viruses/spam and can be deployed as physical or virtual machines. Barracuda followed this up on 30th May 2023 with public disclosure of the issue labelled CVE-2023-2868 - a remote command injection vulnerability with evidence of in-the-wild exploitation, back to at least October 2022.

In their disclosure announcement, Barracuda revealed that they had already released patches on 20th May, which initially seemed more of the same (just another vulnerability, another exploit, and patches to address the issue). However, on 6th June, Barracuda shocked the security industry with an update saying that all impacted devices should be completely replaced (not just patched), irrespective of firmware or patch level. Such a global recall was unprecedented and indicated a problem far more severe and deeply embedded than first thought.

CVE-2023-2868

The CVE itself sounds fairly malicious:

> **CVE-2023-2868**
> A remote command injection vulnerability exists in the Barracuda Email Security Gateway (appliance form factor only) product affecting versions 5.1.3.001-9.2.0.006. The vulnerability arises out of a failure to comprehensively sanitize the processing of .tar file (tape archives). The vulnerability stems from incomplete input validation of a user-supplied .tar file as it pertains to the names of the files contained within the archive. As a consequence, a remote attacker can specifically format these file names in a particular manner that will result in remotely executing a system command through Perl's qx operator with the privileges of the Email Security Gateway product. This issue was fixed as part of BNSF-36456 patch. This patch was automatically applied to all customer appliances.

Mandiant has penned a thorough analysis of the issue for those interested in the more technical aspects:

https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

In brief, when the affected Barracuda appliances receive an email containing an attached 'tar' (Unix/Linux Tape Archive) file, it attempts to extract the contents for further analysis. A flaw in the Barracuda code passes the list of filenames unsanitized as arguments to a system command, giving the attacker control over the command actually executed by manipulating the filenames of files in the archive.

Why so serious?

Exploit of this vulnerability provided attackers with complete control over the affected appliance. As such appliances often contain credentials for access to other network equipment (such as LDAP, FTP, and SMB servers), the attacker can exploit other machines on connected networks using remote access. With full access to the Barracuda appliance, attackers can also install backdoors, proxy tunnels, and a kernel rootkit to compromise the appliance completely.

Given the level of compromise, Barracuda had no choice but to recommend a complete replacement of affected appliances. They simply could not be sure that a simple patch could remove all remnants of all exploits.

While including such a fundamental weakness in a shipping security appliance was undoubtedly careless, Barracuda can be applauded for handling the follow-up in an open and responsive manner.

It is hoped that this event becomes a wake-up call to everyone in the network security community. While we are used to seeing the vulnerability-exploit-patch cycle, we must be aware of other consequences of exploits and how bad they can be.

Network Box 5.5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 5th September 2023, 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 14 days.

Network Box 5 Features
September 2023

This month, for Network Box 5, these include:

- Enhancement to monitoring of mail scanning subsystems
- Performance improvements to mail scanning large HTML documents
- Whitelisting of Microsoft Outlook office scripts (to avoid executable script policy blocks)
- Updating IP range for regional Security Operation Centres
- Renewal of SSL certificates for admin and user portal
- Improvements to LDAP searching and multi-server failover
- Introduce ability to restart IPSEC service from admin web portal
- Allow to set idle timeout for admin web portal and console
- Minor upgrades to SSL VPN package

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 HIGHLIGHTS

SmartLife
Technology Forum 2023

Network Box participated in the **SmartLife Technology Forum**, which took place at the National University of Mongolia. During the event, Network Box Managing Director Michael Gazeley introduced Network Box's Managed Cybersecurity Services to an exclusive list of VIPs.

Global Security Headlines

Bleeping Computer
Akira ransomware targets Cisco VPNs to breach organizations
LINK: https://bit.ly/45QG34F

The Hacker News
Juniper Firewalls, Openfire, and Apache RocketMQ Under Attack from New Exploits
LINK: https://bit.ly/3L8rcu2

Bleeping Computer
FBI warns of patched Barracuda ESG appliances still being hacked
LINK: https://bit.ly/3R5pIUU

Network Box Partnership Agreement Larix Industries Limited

Network Box is pleased to announce a partnership agreement with **Larix Industries** to offer our award-winning Managed Security Services to customers in Mongolia and Kazakhstan.

Newsletter Staff

Mark Webb-Johnson
Editor

Michael Gazeley
Kevin Hla
Production Support

Network Box HQ
Network Box USA
Contributors

Subscription

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