Brace168

January 2020 Newsletter

IN THIS ISSUE:

Author: Lachlan Rodwell – Security Analyst

Brace168 Pty Ltd,

157 Walker St, North Sydney

www.brace168.com

info@brace168.com

P: (02) 9136 6066

> **"Cybersecurity is a shared responsibility, and it boils down to this: in cybersecurity, the more systems we secure, the more secure we all are"**
>
> - Jeh Johnson

Brace168 News!

Brace168 has moved!

Over the holiday period Brace168 moved from our 80 Mount St office to literally just around the corner, at 157 Walker St in North Sydney. Keep an eye out for an eventual office warming party coming very soon.

We've moved to 157 Walker St, North Sydney

Impossible Travel Activity – A Common Alert for Modern Businesses

Brace168 has been reviewing the past couple months' worth of data and has noticed that Impossible Travel Activity is one of the most common alerts received from our clients. Impossible Travel Activity essentially means that a user has logged-in from two different countries within less time than it takes to fly between the countries. This means that if someone halfway across the world tried to use your login credentials after you've already logged in, we would be alerted, and they would be stopped. However, most modern businesses use VPN's for added security, however a VPN could also trigger this alert if you were to set the location to another country. Thus, it is important to distinguish between these two cases so that you get notified when an **incident** has occurred rather than being notified every time an employee uses their VPN and missing the 1% of alerts that actually matter. As this type of alert is so common in most business, this distinction is very necessary for your security. If you're struggling to filter out the noise of alerts, we can help so that you only get notified for the important stuff!

Brace168's thoughts on

Industry News!

Travelex held to ransom in the UK

Reference article: https://www.bbc.com/news/business-51017852

New Year's Eve, a day of celebration for most, was the day hackers launched their attack on the Travelex network. Travelex is a foreign exchange company who you most likely have used to exchange your Australian dollars on holiday. It was later revealed that the hackers had gained access to the network 6 months previously and had in their possession, 5GB of sensitive customer data. They are now holding Travelex to ransom for £4.6 million. The data includes dates of birth, credit card information and insurance numbers.

What is the most shocking is actually the response from Travelex. Upon learning about a breach, in the UK, by law, you have 72 hours to disclose it to the Information Commissioner's Office as well as to customers and business partners, which they did not do. By not complying, they could be forced to pay a fine of 4% of their global turnover.

If you experience a breach, you must notify affected individuals and the Office of the Australian Information Commissioner and failure to comply can lead to fines up to $2.1 million. If you need help complying, we can manage your incident response in compliance with Australian Laws and international standards.

Recent Netflix Phishing Attack

Reference article: https://www.9news.com.au/technology/netflix-email-scam-phishing-scam-mimics-3-step-verification/6ede6c6e-0cbf-4ab5-8797-85d9856e6c0f

Chances are, you have Netflix. Meaning you could be one of the subscribers targeted for a phishing attack sent via email. The attack involves an email pretending to be from Netflix advising you that your "billing information has been modified" and must be updated in the next 24 hours, otherwise your account will be suspended. It even mimics the 3-step verification process to make you think it's genuine!

Rather than watching out for this phishing attack, we would like to remind you to watch out for **all** phishing attacks, as it is one of the most common attacks faced by businesses. If something doesn't feel right, then just simply don't click on it. Think before you click, because no matter how legitimate the attack may seem, there will always be something that doesn't add up.

If your employees need stronger awareness of phishing attacks, we can train them and monitor their emails for suspicious activity so that your employees are secure, and business is protected!

Common Vulnerabilities and Exposure for January

The Top New Vulnerabilities for This Month are:

1. A spoofing vulnerability exists in Windows 10 and Windows Server 2016 in the way that Crypt32.dll validates Elliptic Curve Cryptography (ECC) certificates. An attacker could exploit the vulnerability by using a spoofed certificate to sign a malicious executable and make it appear as if it was from a legitimate and trusted source. (We reported on this last week so check that email for more info)
    - CVE-2020-0601

Score: 8.1

Likelihood: Low – Due to it being discovered relatively quickly, there already being a patch and there is no active exploit, the likelihood of having a device exploited is low. However, the sheer number of devices affected mean that attackers will always be able to find an infected device so update immediately!

Recommendation: Patch to the latest version of Microsoft Windows 10 and Windows Server 2016 as soon as humanly possible!

2. Improper authentication exists in < 12.3.2, < 12.2.6, and < 12.1.12 for GitLab Community Edition (CE) and Enterprise Edition (EE) in the GitLab SAML integration had a validation issue that permitted an attacker to takeover another user's account.
    - CVE-2019-15585

Score: 9.8

Likelihood: Medium – The vulnerability has 14 potential exploits across 6 known affected software configurations, the chance of an exploit is higher. However, since there are no reports of the vulnerability being exploited and denial of service is not possible, the vulnerability does not have a high likelihood, so we are categorising it as a medium. It has also already been patched.

Recommendation: We strongly recommend that all installations running an affected version are upgraded to the latest version as soon as possible.

3. The various versions of Linux consistently have several critical vulnerabilities being discovered. This month, an issue was discovered in Suricata 5.0.0. It is possible to bypass/evade any TCP-based signature by overlapping a TCP segment with a fake FIN packet. Also, a mutation cross-site scripting (XSS) issue in Typora through 0.9.9.31.2 on macOS and through 0.9.81 on Linux leads to Remote Code Execution through Mermaid code blocks, was found. Finally, BFTPD (FTP server) before 5.4 has a heap-based off-by-one error during file-transfer error checking and under certain circumstances, an out-of-bounds read is triggered due to an uninitialized value.
    - CVE-2019-18792
    - CVE-2019-20374
    - CVE-2020-6162
    - CVE-2020-6835

Score: 9.8

Likelihood: Medium – These vulnerabilities all appear to have no active exploits. However, a lot of your systems and devices may run an affected version of Linux without you realising it because so many modern systems use Linux architecture. Thus, there is a higher risk of this vulnerability being exploited due to the nature of most businesses being unaware what Linux operating systems are being utilised in the business.

Recommendation: We would recommend performing a vulnerability scan and from the findings, perform remediation. We regularly perform vulnerability scans so get in contact with us!