Monthly Cybersecurity Newsletter

June 2019 Issue

NC DIT | NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Enterprise Security and Risk Management Office (ESRMO)

From the Desk of the State Chief Risk Officer – Maria Thompson

BlueKeep Vulnerability

The National Security Agency (NSA) has released a cybersecurity advisory for a vulnerability (CVE-2019-0708) called "BlueKeep" that affects several old versions of the Microsoft Windows operating system. The BlueKeep vulnerability allows for an *unauthenticated* attacker to connect to a vulnerable system using the Remote Desktop Protocol (RDP) – formerly known as Terminal Services – and send specially crafted requests without user interaction. An attacker who successfully exploits this vulnerability could then install programs; view, change, or delete data; or create new accounts with full user rights on the vulnerable machine. Microsoft warns that the vulnerability is also "wormable," meaning it can potentially spread from system to system without user interaction.

The "BlueKeep" vulnerability is present in Windows 7, Windows XP, and Server 2003 and 2008. Windows 8 and Windows 10 are not currently vulnerable. Although Microsoft has issued a patch for this vulnerability, potentially *millions* of machines are still vulnerable. Microsoft strongly recommends installing the updates for this vulnerability as soon as possible, after appropriate testing. The update addresses the vulnerability by correcting how Remote Desktop Services (RDS) handles connection requests. In addition to installing the patch, the following steps may also help reduce the risk of this vulnerability.

- Disable RDS if it is not required. Disabling unused and unneeded services reduces exposure to security vulnerabilities.
- Enable Network Level Authentication (NLA) on systems running supported Windows editions. With NLA turned on, an attacker would first need to authenticate to RDS with a valid account on the target system before exploiting the vulnerability.
- Avoid exposing RDP to the public internet. Block TCP port 3389 on the perimeter network firewalls. Blocking this port at the network perimeter firewall will help protect systems that are behind that firewall from attempts to exploit this vulnerability.
- Limit remote session capability to devices that are on the LAN or with VPN access.
- Use multi-factor authentication (MFA).

For more information about BlueKeep, check out the following resources:

- https://www.us-cert.gov/ncas/alerts/AA19-168A

- https://www.nsa.gov/Portals/70/documents/what-we-do/cybersecurity/professional-resources/csa-bluekeep_20190604.pdf?ver=2019-06-04-123329-617
- https://blogs.technet.microsoft.com/msrc/2019/05/30/a-reminder-to-update-your-systems-to-prevent-a-worm/

Hurricane-Related Scams

The 2019 hurricane season has arrived, and both North Carolina State University and the Weather Company predict this could be a slightly above average season. As if the weather were not enough to concern us, natural disasters come with cyber threats. Criminals love to take advantage of these disasters and other people's misfortunes. The Cybersecurity and Infrastructure Security Agency (CISA) warns us to remain vigilant for malicious cyber activity targeting disaster victims and potential donors. Fraudulent emails commonly appear after major natural disasters and often contain links or attachments that direct users to malicious websites. Individuals should exercise caution in handling any email with a hurricane-related subject line, attachments, or hyperlinks. In addition, users should be cautious of social media pleas, texts, or door-to-door solicitations relating to severe weather events. To avoid becoming victims of this type of malicious activity, take the following steps:

- Carefully review email and web addresses since cybercriminals will make them look as legitimate as possible, often using variations of spellings. The URL may have a different domain, such as *.gov* instead of *.net*.
- Do not click on links in emails from anyone unless you know and have verified the sender of the email.
- Take time to review the sender's email address. Do not click on any links until you are certain the organization is real. Check the organization's website for its contact information, and use sites such as www.charitynavigator.org to verify a charity organization.
- Make sure all your anti-virus software is up to date, and you have enabled the anti-phishing software provided by your email client.
- Criminals send phishing emails and make phone calls posing as official representatives of disaster aid organizations, such as FEMA. A true FEMA representative will never ask for personal banking information, a Social Security number, or a registration number.

For more information about dealing with weather emergencies and avoiding disaster scams, check out the Federal Trade Commission's Consumer Information on Dealing with Weather Emergencies: https://www.consumer.ftc.gov/features/dealing-weather-emergencies.

If you believe you have been a victim of cybercrime, file a complaint with the Federal Bureau of Investigation Internet Crime Complaint Center at www.ic3.gov.

INTERNET CRIME COMPLAINT CENTER
www.ic3.gov

Detecting a Phishing Email

LogRhythm Labs

10 Things to Watch

With the uptick in ransomware infections that are often instigated through phishing emails, **it's crucial to take proactive measures to help protect yourself and your organization's security.**

Having a computer that is up to date and patched makes a big difference in reducing an organization's overall risk of infection.

But being vigilant in detecting phishing emails and educating employees in your organization to also be proactive is a critical step in protection.

Here is a quick top ten list for how to spot and handle a phishing email.

1 Don't trust the display name of who the email is from.

Just because it says it's coming from a name of a person you know or trust doesn't mean that it truly is. Be sure to look at the email address to confirm the true sender.

2 Look but don't click.

Hover or mouse over parts of the email without clicking on anything. If the alt text looks strange or doesn't match what the link description says, don't click on it—report it.

3 Check for spelling errors.

Attackers are often less concerned about spelling or being grammatically correct than a normal sender would be.

4 Consider the salutation.

Is the address general or vague? Is the salutation to "valued customer" or "Dear [insert title here]?

5 Is the email asking for personal information?

Legitimate companies are unlikely to ask for personal information in an email.

6 Beware of urgency.

These emails might try to make it sound as if there is some sort of emergency (e.g., the CFO needs a $1M wire transfer, a Nigerian prince is in trouble, or someone only needs $100 so they can claim their million-dollar reward).

7 Check the email signature.

Most legitimate senders will include a full signature block at the bottom of their emails.

8 Be careful with attachments.

Attackers like to trick you with a really juicy attachment. It might have a really long name. It might be a fake icon of Microsoft Excel that isn't actually the spreadsheet you think it is.

9 Don't believe everything you see.

If something seems slightly out of the norm, it's better to be safe than sorry. If you see something off, then it's best to report it to your security operations center (SOC).

10 When in doubt, contact your SOC.

No matter the time of day, no matter the concern, most SOCs would rather have you send something that turns out to be legit than to put the organization at risk.

CYBERSECURITY NEWSLETTERS

Security Awareness Newsletter: Monthly security awareness newsletter provided by KnowBe4 for all State employees.
***Note**: You must have a valid State employee O365 account.*

- https://ncconnect.sharepoint.com/sites/it_ext/esrmo_ext/Documents/Newsletters/Security%20Awareness%20News/2019

Security Tips Newsletter: Free monthly cybersecurity resource from the Center for Internet Security (CIS). This month the newsletter covers ***Staying Cyber-safe on a Summer Vacation***.

- https://www.cisecurity.org/resources/?type=newsletter

SANS OUCH! Newsletter: Free monthly cybersecurity awareness newsletter provided by The SANS Institute. This month's edition is titled ***Dark Web.***

- https://www.sans.org/security-awareness-training/ouch-newsletter

ISSA Web CONFERENCES

Security Standards Organizations Webinar

Security Standards Organizations – The good, the bad, and the ugly? This webinar will cover the evolution of several technologies to address the evolving threat models. Changes to the SOC and response technologies will be included.

Date / Time: **July 23, 2019 @ 12:00 pm**

For more information and to register for this event, click here.

In this webinar, **Perry Carpenter, Chief Evangelist and Strategy Officer for KnowBe4**, dives into ideas like how to use "Trojan Horses for the Mind," how to leverage social dynamics to drive behavior and shape culture, and unveils some exciting new behavior models that will help you stop the bad guys in their tracks. Click here to view this webinar.

July's Cyber Awareness Training Oppotunities

July is a busy month for many state employees. In addition to fiscal year close outs, this is the season for summer camps, traveling and family vacations. We are most vulnerable in this time, as we sometimes forget key security practices we use throughout the year at work. We attempt to separate our work behavior from our home life, but we forget that the cyber risks we experience in our work life are also present in our home life. Generally speaking, hackers tend to look for low-hanging fruit as the first level to attack. It is therefore important that we adopt the model to be good stewards of ALL sensitive data, at ALL times. Make yourself a **HARD TARGET** by doing the following:

- Use strong passwords and passphrases.
- Use Multi-Factor Authentication (MFA) solutions.
- Use a Virtual Private Network (VPN) to access sensitive systems and data.
- Take that extra time to verify whether emails are legitimate.
- Stay abreast of emerging threats, tactics and techniques.

On **July 1, 2019**, ESRMO will release the third cybersecurity training module called "How to Be a Human Firewall!" to all users. Firewalls and antivirus and information security technology are helpful, but protecting sensitive data is still a human process. Learn what it means to become a **human firewall**.

Role-Based Training Courses

Those who have been assigned duties as Database Administrators and Application Developers will also be assigned the ROLE-BASED courses listed below.

- Privileged User Security Series: Secure Database Administration
- Secure Coding Series: Introduction to Web Application Security

Note: The Role-Based Training courses will NOT be delivered through the State LMS but through the training vendor portal (KnowBe4). Only those employees whose names were submitted by the agency will receive this courseware.

Duration: 7-28 minutes (varies per course)
Due Date: August 15, 2019

- **June** – National Safety Month (NSM)
- **July 1** – Formal kick-off of annual BC/DR Plan reviews by agencies; runs July 1 through October 31
- **July 4** – Independence Day
- **July 18** – Data Connectors Raleigh Cybersecurity Conference
- **September 1** – Agency Compliance Reports Due
- **September 2** – Labor Day