NJCCIC

NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

THE WEEKLY BULLETIN | September 9, 2015

Joint Advisory Bulletin

September 8, 2015

Mobile Payment System Vulnerability

The U.S. Secret Service has observed a steady increase in criminals exploiting vulnerabilities in the account provisioning and verification process for near field communication (NFC) payments to commit fraud. Specifically, criminals are using stolen identity information (e.g., credit reports, tax records, healthcare and employee records that contain personally identifiable information) to establish fake accounts on NFC devices and make illicit transactions both online and at "brick and mortar" retailers. Over the last several months, perpetrators have conducted numerous fraudulent transactions using this particular method of exploitation affecting many high-end retailers and banking institutions across the Northeastern portions of the United States.

Latest Cyber Alerts

Multiple Vulnerabilities in PHP Could Allow Arbitrary Code Execution

Vulnerability in Windows Media Center Could Allow Remote Code Execution

Cumulative Security Update for Internet Explorer

Multiple Vulnerabilities in Microsoft Windows Journal Could Allow Remote Code Execution

Cumulative Security Update for Microsoft Edge

Vulnerabilities in .Net Framework

Vulnerabilities in Microsoft Office

Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution

Multiple Vulnerabilities in Adobe Shockwave Player

Tip of the Week

"Beware of Rogue Anti-Virus Software"

NJCCIC Announcements

In Case You Missed It:

Rogue software or "scareware" is fake antivirus or security software. Bad actors usually try to get you to install it by generating a pop-up window as you surf the web. The "updates" or "alerts" in the pop-up windows request you to take some sort of action, such as clicking to install the software, accept recommended updates, or remove unwanted viruses or spyware. When you click, the rogue security software downloads to your computer.

NJCCIC analysts discussed what cyber threats and security concerns that continue to dominate the news as data breaches, doxing attacks, and other methods target government, private sector and individual victims in the lastest OHSPwebinar.

Listen to webinar here

Last Chance:

Registration for September 16-17 cybersecurity workshop ends today.

Save your spot and learn more about the workshop here.

Connect with us!

---

cyber.nj.gov

New Jersey Cybersecurity & Communications Integration Cell