NJCCIC

NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

THE WEEKLY BULLETIN | December 23, 2015

Cyber Alert: Critical Vulnerabilities in Juniper Networks ScreenOS

On December 17, Juniper Networks, a network solutions provider, revealed that an internal code review uncovered that its ScreenOS NetScreen firewall contained extraneous code, also described as a "backdoor," potentially allowing attackers to gain unauthorized remote administrative access to NetScreen devices as well as to decrypt Virtual Private Network (VPN) traffic on the firewalls. The unauthorized code, injected approximately three years ago and only recently discovered, could allow attackers to gain access to encrypted communications using a valid username and the backdoor password, which was publically revealed by security researchers on Sunday. Juniper customers are urged to patch immediately. Read more.

Phishing Alert: Unpaid Invoice & Order Confirmation Phishing Emails

As the year comes to a close, the NJCCIC reminds our members that phishing emails continue to be the most widely used and effective method of infecting organizations with malware, from ransomware and exploit kits to sophisticated Trojans and worms. Over the last year, malicious emails with "invoice" attachments were particularly effective at infecting businesses across the country, as these emails commonly targeted employees who regularly receive and pay invoices. Malicious actors are also capitalizing on the holiday shopping season, sending unsolicited "order confirmation" emails requiring users to open a link or attachment to complete an order or confirm shipping details. For more information and recommendations, read more.

Breach Notification

Landry's Inc.

On December 17, Landry's Inc. announced it

Latest Cyber Alerts

Vulnerabilities in Juniper ScreenOS

Vulnerability in Apache Commons

was investigating a potential point-of-sale breach after unauthorized charges were detected on cards used at some of their restaurant locations. Landry's owns and operates over 500 restaurants nationwide, including Landry's Seafood, Chart House, Rainforest Cafe, Morton's, and McCormick & Schmick's. The company is not yet aware of the specific locations involved in the breach.

Hello Kitty - SanrioTown

On December 19, a security researcher revealed a vulnerability in a database housing 3.3 million Hello Kitty customer accounts, potentially exposing personal information including full names, birthdays, gender, country of origin, email addresses, unsalted password hashes, password hint questions, and their corresponding answers. The vulnerable database also contained information on 186,261 children under the age of 18. Though the Hong-Kong based company stated there is no evidence any customer data was stolen, users are encouraged to change passwords and security questions.

Collections - Update

Uninstalled Outdated Versions of Java Pose Security Risk

Cyber News

Congress Approves First Major Cyber Bill in Years
via The Hill

AP Investigation: US Power Grid Vulnerable to Foreign Hacks
via Associate Press

Iranians Hacked Into New York Dam
via CNN

Russian Government Likely Behind APT 28
via SC Magazine

Cisco Reviews Code After Juniper Breach; More Scrutiny Expected
via Reuters

Questions?

Email a Cyber Liaison Officer at njccic@cyber.nj.gov.

Connect with us!

cyber.nj.gov

New Jersey Cybersecurity & Communications Integration Cell

DISCLAIMER: This bulletin is provided as is for informational purposes only. The New Jersey Cybersecurity & Communications Integration Cell (NJCCIC) and the Regional Operations Intelligence Center (ROIC) do not provide any warranties of any kind regarding any information contained within. The NJCCIC and ROIC do not endorse any commercial product or service, referenced in this bulletin or otherwise. Further dissemination of this bulletin is governed by the Traffic Light Protocol (TLP). For more information about TLP, see https://www.us-cert.gov/tlp/.