NJCCIC

NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

THE WEEKLY BULLETIN | February 19, 2016

Alert: Vulnerability in GNU C Library Could Allow for Remote Code Execution

A buffer overflow vulnerability (CVE-2015-7547 and CWE-121) has been identified in the GNU C Library (glibc) DNS resolver that could allow a remote attacker to execute arbitrary code. The vulnerable code was initially added in 2008 and affects all versions from version 2.9, released in November 2008, to version 2.22. The glibc client side DNS resolver is vulnerable to a stack-based buffer overflow when using the getaddrinfo() library. This vulnerability may be exploited through attacker-controlled DNS servers or domain names, or through man-in-the-middle attacks. Read more here.

New Info Sharing Guidance

On February 16, 2016, the Department of Homeland Security (DHS) released a series of documents outlining procedures to share and disseminate cybersecurity information. The Automated Indicator Sharing (AIS) initiative developed by the DHS, enables timely sharing of cyber threat indicators between federal entities, non-federal entities, and the private sector. The goal of the AIS initiative is to share real-time cyber threat indicators through the National Cybersecurity and Communications Integration Center (NCCIC), receive indicators from the private sector and other entities, remove any

Latest Cyber Alerts

Multiple Vulnerabilities in Mozilla Firefox Could Allow for Arbitrary Code Execution

Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

Vulnerability in AMX Harman Professional Devices Could Allow Unauthorized Remote Access (Updated)

Tip of the Week

"EMV 101"

If retail stores offer the option to swipe or insert your card, always choose to insert your

personally identifiable information, and disseminate indicators as appropriate. This initiative was developed as directed by the Cybersecurity Information Sharing Act of 2015 signed into law on December 18, 2015 by President Obama. Read more here.

chip-and-PIN card for increased security! Read more here.

NJCCIC *at a glance*

Opinion: Why Cybersecurity Needs a Grass-Roots Solution

NJCCIC Comment: With ever-increasing cyber attacks launched against businesses, organizations, and governments, it's evident that cybersecurity is in need of a real grass-roots solution to propel progress. New Jersey's own Director of Cybersecurity, Dave Weinstein, weighs in on the discussion, highlighting the benefits of information sharing and promotion of best practices between federal government, state and local government, and industry.

Apple CEO opposes court order to help FBI unlock iPhone

NJCCIC Comment: Apple's uncompromising stance has further stoked the public debate over whether or not privacy and security are mutually exclusive, potentially paving the way to the US Supreme Court. The court order would require Apple to develop a firmware update which would allow investigators to bypass the limitation of 10 passcode attempts in order to avoid wiping all data from the device used by the San Bernardino shooter.

CIA Director John Brennan on 60 Minutes

NJCCIC Comment: The CIA director underscored the seriousness of the cyber threat to US critical infrastructure, stating it "really is the thing that keeps me up at night." The Director went on to explain that those who possess the capability to turn off the lights in the United States, currently do not have the intent to do so.

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/.