



NJCCIC

NJ CYBERSECURITY & COMMUNICATIONS INTEGRATION CELL

THE WEEKLY BULLETIN | July 21, 2015

Recent Threat Analysis

July 21, 2015

[Critical Infrastructure: Vulnerabilities Increasing. Risks High](#)

Critical infrastructure sites are increasingly vulnerable to cyberattack as the systems that run them become more accessible, interconnected, and reliant on cyberspace. The risks posed to Industrial Control System and Supervisory Control and Data Acquisition (ICS/SCADA) systems will continue to heighten as new and existing vulnerabilities are exploited by both criminal and state-sponsored threat actors.

July 20, 2015

[Vulnerability Microsoft Font Driver For Windows Server 2003](#)

An out-of-band patch was released for Microsoft Operating Systems that addressed a vulnerability in Microsoft Font Driver that could allow arbitrary code execution (CVE-2015-2426). The patch did not address Windows Server 2003 as it is no longer supported publicly by Microsoft, however, this vulnerability does affect Windows Server 2003.

Latest NJCCIC Alerts

[Vulnerability in Adobe Shockwave Player Could Allow for Arbitrary Code Execution](#)

[Multiple Vulnerabilities in Adobe Reader and Adobe Acrobat Could Allow Remote Code Execution](#)

[Vulnerability in Microsoft Remote Desktop Protocol Could Allow for Remote Code Execution](#)

[Vulnerability in Microsoft Office Could Allow Remote Code Execution](#)

[Cumulative Security Update for Internet Explorer](#)

NJ Cyberlog

The NJCCIC's blog, "[NJ Cyberlog](#)," is live!

Keep an eye on our website and follow us on Twitter to read the latest thought leadership from our team.

[Read The Inaugural Post Here](#)

NJCCIC Announcements

Tip of the Week

"Use Anti-Virus Software"

Virus authors continuously release new and updated viruses.

Set your Anti-Virus software to scan your system automatically. Manually scan files you receive before opening them. These include files you download from the internet, email attachments, and files on USB drives and other media.

The NJCCIC's Analysis Branch consists of dedicated cyber threat intelligence analysts with sector-specific portfolios.

Contact a Cyber Liaison Officer at njccic@cyber.nj.gov with any Requests for Information (RFIs) or to arrange for sector-specific threat briefings.

Questions?

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

Connect with us!



www.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 and 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 advisory or otherwise. Further dissemination of this advisory is governed by the Traffic Light Protocol (TLP). For more information about TLP, see <http://www.us-cert.gov/tlp/>.

Share this email:



Got this as a forward? [Sign up](#) to receive our future emails.

View this email [online](#).

communications@njohsp.gov

Trenton, NJ | 08625 US

This email was sent to kmiscia@montclairnjusa.org.

To continue receiving our emails, add us to your address book.

