

*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**TLP: WHITE**

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

<http://www.us-cert.gov/tlp/>

**DATE(S) ISSUED:**

12/17/2015

**SUBJECT:**

Vulnerability in FireEye Products Could Allow for Remote Code Execution

**OVERVIEW:**

A vulnerability has been discovered in FireEye NX, EX, FX and AX Series products that could allow for remote code execution. The vulnerability exists in how the Malware Input Processor (MIP) module analyzes Java (.jar) files. Successful exploitation could lead to network surveillance activity, root access on the device, privilege escalation, and information disclosure.

**THREAT INTELLIGENCE:**

There are currently no reports of this vulnerability being exploited in the wild.

**SYSTEMS AFFECTED:**

- EX Prior to Security Content Version 427.334
- NX Prior to Security Content Version 427.334
- AX Prior to Security Content Version 427.334
- FX Prior to Security Content Version 427.334

**RISK:**

**Government:**

- Large and medium government entities: **High**
- Small government entities: **High**

**Businesses:**

- Large and medium business entities: **High**
- Small business entities: **High**

**Home Users: N/A**

**TECHNICAL SUMMARY:**

A vulnerability has been discovered in FireEye NX, EX, FX and AX Series products that could allow for remote code execution. The vulnerability exists in how the Malware Input Processor (MIP) module analyzes Java (.jar) files.

In order to exploit this vulnerability an attacker would have to send an email with a malicious Java (.jar) attachment or convince a user to follow a link to gain access to the device. In some cases, the recipient would not have to read the email, as receiving it would be sufficient to exploit the vulnerability. Successful exploitation could lead to network surveillance activity, root access on the device, privilege escalation, and information disclosure.

FireEye customers configured for automated security updates, should have received the security content update on 12/5/2015. FireEye is also providing support for out-of-contract customers. These customers should contact the FireEye support team at [support@fireeye.com](mailto:support@fireeye.com).

#### **RECOMMENDATIONS:**

The following actions should be taken:

- Apply appropriate patches provided by FireEye to vulnerable systems.
- Enable automatic updates for Security Content on vulnerable systems.
- Restrict access to the physical and management interfaces to authorized personnel and authorized hosts.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

#### **REFERENCES:**

##### **FireEye:**

<https://www.fireeye.com/content/dam/fireeye-www/support/pdfs/fireeye-rce-vulnerability.pdf>

##### **ZDNet:**

<http://www.zdnet.com/article/googles-project-zero-uncovers-critical-flaw-in-fireeye-products/>

**TLP: WHITE**

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

<http://www.us-cert.gov/tlp/>