Security Advisory

September 2, 2016

FireEye recently worked with Riot Games to address an identified evasion as part of our vulnerability disclosure program. On April 27th, 2016 FireEye was informed of an evasion that impacted the NX Series products. On April 28th, 2016, FireEye released fixes via automated security content updates to resolve the issue.

FireEye Label: Evasion
Credit: Riot Games
Researcher Reference: Jason Clark
Severity: Medium
Products Affected: NX 1300, NX 2300 and NX 4300
Description:

An evasion existed that would allow an attacker to bypass FireEye detection. The issue has been remediated.

Version and Fix Details:

Product	Fixed Version	Date Released	Customer Actions Required
NX	SC 483.134	04-28-2016	Update to the latest version

We appreciate the support of the security researcher community and encourage responsible disclosure of any potential security issues. We encourage all FireEye customers to leverage security best practices (provided below) where possible in their environments to continue to limit security risk exposure.

FireEye Security Best Practices

- Always keep the product version up-to-date
- Limit network access to the management interface(s) of the appliance with firewalls or similar measures
- Only issue accounts to trusted administrators
- Utilize strong passwords
- Monitor logs
- Restrict physical access to the appliance to trusted administrators

To report vulnerabilities in FireEye products, please send an email to security@FireEye.com.

Revision history:

Version	Date
Version 1	September 2, 2016

If you have any questions, please contact FireEye Support at support@fireeye.com or 877 347-3393 (877-FIREEYE) or 408 321-6300.

For further information, Please visit our Customer Support page at:

http://www.fireeye.com/support/contact-customer-support.html