FireEye Statement about OpenSSL "Heartbleed" Vulnerability: CVE-2014-0160

The "Heartbleed" vulnerability (CVE-2014-0160) potentially allows attackers to access confidential data within the memory space of services and applications using vulnerable versions of OpenSSL. Detailed information about the vulnerability can be found from a number of sources, including:

http://heartbleed.com

https://www.openssl.org/news/secadv_20140407.txt

FireEye is in the process of assessing all products and services within our portfolio. Here is the current status of each:

Assessed, Patched:

- Endpoint Security (HX Series) - formerly known as Mandiant for Security Operations (MSO): Patched on Wednesday, April 16th
- Mandiant Intelligent Response 3.x and later: Patched on Wednesday, April 16th

Assessed, Not Vulnerable:

- Web Security (NX Series)
- Email Security (EX Series)
- Content Security (FX Series)
- Forensic Analysis (AX Series)
- Central Management (CM Series)
- Email Threat Prevention Service
- Mobile Threat Prevention Service
- Dynamic Threat Intelligence
- Managed Defense Portal
- Mandiant Intelligent Response 2.x (and earlier)
- Threat Analytics Platform
- Mandiant Intelligence Center
- Mandiant Cloud Alert

Additional information may be posted as it becomes available.

For further information, contact Mandiant Customer Service.

https://support.mandiant.com

support@mandiant.com

U.S./Canada: +1 (877) 962-6342

Worldwide: +1 (703) 637-9377