VISA SECURITY ALERT

April 2014

OPENSSL 'HEARTBLEED' VULNERABILITY

Distribution: Merchants, Issuers, Acquirers, Processors

Who should read this: IT, Information Security, Risk Management

Summary

On April 8, 2014 the US-CERT issued an alert pertaining to a critical vulnerability in OpenSSL (CVE-2014-0160). The OpenSSL 'Heartbleed' vulnerability has the potential to affect significant portions of the payment ecosystem. Due to the critical nature of this vulnerability, Visa is encouraging clients to not only apply a patch, but also understand that OpenSSL secret (private) keys generated under vulnerable versions of the software should be regarded as compromised and must be regenerated on affected systems and hardware.

Description and Impact

This vulnerability affects versions 1.0.1 – 1.0.1f and 1.0.2 – beta of OpenSSL. The vulnerability could potentially be exploited to disclose sensitive private information to an attacker, including:

- Primary key material (secret keys)
- Secondary key material (user names and passwords used by vulnerable services)
- Protected content (sensitive data used by vulnerable services)
- Collateral (memory addresses and content that can be leveraged to bypass exploit mitigations)

OpenSSL is used on many systems within the payment ecosystem, typically on servers that terminate TLS/HTTPS connections. Web servers, VPN concentrators, SSL terminators, and systems used to communicate with PIN Entry Devices (PEDs) all commonly involve an implementation of OpenSSL. As the vulnerability is regarded as critical, Visa clients, as well as their agents and merchants, are strongly advised to patch all affected systems as soon as possible (PCI DSS requirement 6.2 requires patching within one month). The vulnerability allows a malicious attacker to extract secret keys and security credentials from the memory of the affected system. Clients and merchants must therefore regard such secret keys as compromised and regenerate keys accordingly.

According to US-CERT, exploit code is publicly available for this vulnerability and it is expected that attacks are already underway.

Mitigation

This Visa Security Alert is provided for information purposes only. Clients and merchants are advised to ensure that systems affected by this vulnerability are not only patched but that all secret keys are regenerated and deployed on affected devices and systems.

- **Patch vulnerable OpenSSL versions as quickly as possible**. OpenSSL 1.0.1g has been released to fix this vulnerability. Although PCI DSS requirements state patching must occur within one month, Visa highly recommends applying the patch for this vulnerability as soon as possible.

- **Generate and deploy new SSL keys.** Keys generated with a vulnerable version of OpenSSL should be considered compromised and regenerated with the patched version. SSL keys will then need to be redeployed to address the vulnerability.

Additional Resources

Further details are provided in the US-CERT alert: http://www.us-cert.gov/ncas/alerts/TA14-098A

To report a data breach, contact Visa Fraud Control:

- Asia Pacific Region, Central Europe/Middle East/Africa Region: VIFraudControl@visa.com

- Canada Region, Latin America Region, United States: USFraudControl@visa.com

For more information, please contact Visa Risk Management: cisp@visa.com