Security Vulnerability
"Hearbleed" OpenSSL
US-CERT CVE-2014-0160

"Heartbleed" – US-CERT (CVE-2014-0160): Informational Guidance

This document has been prepared in order to provide information and guidance with respect to the recently uncovered OpenSSL security vulnerability referred to as "Heartbleed".

SERVICE IMPACT

None of your Allied Telecom Group provided services were, or are, vulnerable to this OpenSSL flaw, therefore no action is required with respect to your Allied services. In the interest of providing you with information of value, we have prepared this guidance to assist you in ascertaining your overall exposure.

SYNOPSIS

The OpenSSL "Heartbleed" vulnerability, identified by US-CERT (CVE-2014-0160) is a critical flaw in OpenSSL Software. OpenSSL is a popular, and widely deployed, software used to secure websites, and other (typically network based) applications and services. OpenSSL software is employed in application specific network appliances, as well as other embedded systems. Organizations and Individuals that rely on OpenSSL software to protect (through encryption) data, should take appropriate steps to mitigate this vulnerability, and further minimize or eliminate future exposure. Failure to mitigate this vulnerability places all sensitive data, otherwise secured by OpenSSL software, at risk.

Approximately two-thirds of all web servers use OpenSSL software. As such, a compelling statistical likelihood exists that all Organizations and/or Individuals have been affected by this (somewhat) minor programatic error.

SCOPE

The "Heartbleed" vulnerability, while discovered recently, has been in existence for in excess of Two(2) Years. During this vulnerability window, the potential exists that all data secured via (vulnerable versions of) OpenSSL software, were at risk of being compromised at some level.

It is important to note, due to the nature and duration of this vulnerability, the following technical aspects, in order to assist in the assessment of your overall exposure:

- Exploitation of this vulnerability leaves no trace or evidence of compromise.
- If a service was compromised at any time during the vulnerability window (in excess of Two (2) Years), any/all data (that was captured) from said service should be considered compromised. Meaning: If Encrypted data was captured PRIOR to the service being compromised, once compromised the hacker could replay and decrypt previously captured data.

Any/all data from a compromised service should be considered compromised for the entire vulnerability window, up to the point where the Encryption Keys are changed. ***NOTE:*** *Even after Encryption Keys are changed, all previously captured data using compromised Encryption Keys should still be considered compromised.*

REPRESENTATIVE EXAMPLE

A Web Server subject to this vulnerability could have been requested to reveal random bits of Server Memory Data over and over and over again. Inadvertently, said Web Server 'COULD' send its Encryption Keys (as random bits of data). ***NOTE:*** *OpenSSL software is designed to protect Encryption Keys from being exposed in this manner, however, as a result of a programming error, this built-in protection mechanism was circumvented.*

Once the Encryption Keys have been compromised, the attacker/hacker can monitor all communications to/from the compromised Server in its un-encrypted form. This allows access to sensitive data such as, but not limited to: account numbers, usernames, passwords, credit-card numbers, etc. Additionally, skilled hackers could create fake versions of trusted sites capable of fooling browser software and users alike.

What makes this vulnerability most troubling is the fact that all of the above can be accomplished without leaving a trace. As a direct result, it's nearly (if not completely) impossible to determine the extent of damage caused by the "Heartbleed" vulnerability.

RECOMMENDED CORRECTIVE ACTION

Consult with your IT Staff to determine if any IT Systems, such as Website(s), eMail Servers, Networks, VPN Concentrators, etc. utilize OpenSSL software. Up-to-date vulnerability details, including a number of solutions can be obtained at heartbleed.com

All systems utilizing (at least affected versions of) OpenSSL software should be immediately upgraded to the latest (unaffected) OpenSSL software version. v1.0.1g as of this writing.

NOTE: *Verify/Validate all 'Embedded Systems' e.g. VPN Concentrators, Firewalls, Secure Routers, etc. Please also note that certain softwares 'incorporate' OpenSSL into the final application. Due to licensing considerations any such 'incorporation/inclusion' should be clearly identified in the applications license or other documentation.*

If you have affected systems, the following steps are recommended for discussion and/or implementation with your IT Team:

- **Update** OpenSSL systems to the latest version of OpenSSL (and reboot system)
- **Generate new Encryption Keys** (per your systems procedure/instructions)
- **Obtain a Replacement/New SSL Certificate** from a trusted Certificate Authority(CA)
- **Notify Employees**, raising awareness of this issue and providing guidance.
- **Notify Employees and Customers** of your actions with respect to this vulnerability.
- Once all affected systems have been identified and re-secured; inform your Employees and Customers to **change** their **passwords** for any affected system(s).
- **Notify Employees and Customers** that if they utilize the same username and/or password combination on other systems, that they should change those passwords as well.
- **Confer with business partners, contractors, service providers, etc...** to identify any/all possible exposures in their systems, and the steps being taken to mitigate same.
- Understand that even if your business does not utilize OpenSSL, it is likely that non-business **personnel accounts** have been impacted by "Heartbleed." For such accounts it is recommended that you DO NOT log in to those sites/accounts until you are certain that the provider in question has addressed this vulnerability. If vulnerability information is not clearly posted (on the log-in screen), it is recommended that you contact the providers support activity.
- Upon confirming that a provider has mitigated this threat, you should then log-in and **change** your **password**.
- Going forward, it is recommended that you **monitor financial accounts** (bank, credit-card, etc) for unrecognized/unauthorized changes to those accounts. Most specifically over the next several weeks.

Source 'US-CERT' Advisory Notice

US-CERT - (CVE-2014-0160)

SYSTEMS AFFECTED

- OpenSSL 1.0.1 through 1.0.1f
- OpenSSL 1.0.2-beta

OVERVIEW

A vulnerability in OpenSSL could allow a remote attacker to expose sensitive data, possibly including user authentication credentials and secret keys, through incorrect memory handling in the TLS heartbeat extension.

DESCRIPTION

OpenSSL versions 1.0.1 through 1.0.1f contain a flaw in its implementation of the TLS/DTLS heartbeat functionality. This flaw allows an attacker to retrieve private memory of an application that uses the vulnerable OpenSSL library in chunks of 64k at a time. Note that an attacker can repeatedly leverage the vulnerability to retrieve as many 64k chunks of memory as are necessary to retrieve the intended secrets. The sensitive information that may be retrieved using this vulnerability include:

- 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)

Exploit code is publicly available for this vulnerability.

Additional details may be found in CERT/CC Vulnerability Note VU#720951.

IMPACT

This flaw allows a remote attacker to retrieve private memory of an application that uses the vulnerable OpenSSL library in chunks of 64k at a time.

SOLUTION

OpenSSL 1.0.1g has been released to address this vulnerability. Any keys generated with a vulnerable version of OpenSSL should be considered compromised and regenerated and deployed after the patch has been applied.

US-CERT recommends system administrators consider implementing Perfect Forward Secrecy to mitigate the damage that may be caused by future private key disclosures.

REFERENCES

- OpenSSL Security Advisory
- The Heartbleed Bug
- CERT/CC Vulnerability Note VU#720951
- Perfect Forward Secrecy
- RFC2409 Section 8 Perfect Forward Secrecy