Heartbleed SSL Vulnerability

Information Security and Information Technology personnel need to test their systems immediately to see if they are vulnerable to this issue.

Q.) What is this vulnerability?

A.) In a vulnerability that has been described as the Heartbleed bug, a missing bounds check in the handling of the TLS heartbeat extension can allow remote attackers to view up to 64 kilobytes of memory on an affected server. This vulnerability could enable attackers to retrieve private keys and ultimately decrypt the server’s encrypted traffic or even impersonate the server. Attackers could also potentially recover usernames and passwords from the acquired system memory.

Q.) What versions of the OpenSSL library are affected?

• OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable
• OpenSSL 1.0.1g is NOT vulnerable
• OpenSSL 1.0.0 branch is NOT vulnerable
• OpenSSL 0.9.8 branch is NOT vulnerable
The Bug was introduced to OpenSSL in December 2011 and has been out in the wild since OpenSSL release 1.0.1 on 14th of March 2012. OpenSSL 1.0.1g released on 7th of April 2014 fixes the bug.

Affected systems include web servers, payment gateways, webmail systems, web portals, VPN systems, and other SSL enabled devices and sites.

Proof of concept code has been posted online and is available.

How serious is this bug?

Potentially quite serious, though the bug has existed since December 2011.

Managers and administrators should make a focused and prioritized effort to identify and upgrade or patch vulnerable systems within their environment.

Additionally, vulnerable systems may exist with third parties used by your firm, including webmail, training portals, online banking, etc..
How can I test my systems to learn if they are vulnerable?

Online tools to conduct tests exist at the following sites:

https://www.ssllabs.com/ssltest/
http://filippo.io/Heartbleed/
http://possible.lv/tools/hb/

Recommendations to remediate this Vulnerability:

1. Be thorough in testing all potentially vulnerable systems in the enterprise - not just those that are externally facing.
2. Conduct an inventory all systems and servers running OpenSSL 1.0.1 and newer
3. Upgrade to OpenSSL 1.0.1g or recompile with -DOPENSSL_NO_HEARTBEATS.
4. Revoke potentially compromised SSL keys and reissue new keys from the Certificate Authority
5. Change all user passwords and encryption keys on any vulnerable enterprise applications or systems. Also change user credentials on 3rd party systems that may have been vulnerable.
6. All session keys and session cookies must be expired/invalidated
7. All users of systems where SSL is in use must be informed of the potential for compromise

Beyond these technical steps, companies should consider the following best practices:

1. Consider engagement with security professionals to regularly assess the security of enterprise networks, systems, and applications. Penetration tests and Security Posture Assessments provide early opportunity to discover security vulnerabilities and weakness and to close gaps before they are exploited by attackers.
2. Assign a project manager and ensure that the discovery, testing, and remediation of this vulnerability is thorough and successfully completed.
3. Ensure that newly purchased, configured, or installed systems and appliances are tested against this vulnerability as part of your vulnerability management program - prior to go-live of the new site or system.
4. Audit proactively and regularly to ensure that user credentials have been changed. Compare current credential hashes with those used previously by users to ensure that vulnerable credentials do not exist.

WHERE SHOULD THE PRIORITY FOCUS BE?

Ensure that all systems involving sensitive data and financial transactions, and systems providing remote access (VPN’s, etc) are tested first. Then test main web sites and portals.