April 10, 2014

To: IT Executives and Security Staff

CRITICAL Vulnerability In OpenSSL: HeartBleed

The REN-ISAC [1] wants to stimulate immediate action concerning a CRITICAL vulnerability in a pervasive piece of software, and make itself available for questions and assistance in understanding how to deal with the issue.

OpenSSL is an open-source implementation of the SSL and TLS [2] protocols. SSL/TLS provides the cryptographic function for almost all secure Internet communications. One most obvious example is secure web services. OpenSSL is widely utilized in open-source and commercial products. The odds are certain that your enterprise relies on OpenSSL-based services.

The HeartBleed bug in OpenSSL is simple and easily exploited. A "heartbeat" mechanism in the protocol allows a client to tell a server "I'm going to send you some data, echo it back to me". The client's request contains the data and specifies the length of the data. If the specified length is larger than the length of the data sent, the server returns an amount of data equal to the specified length with contents of server process memory making up the difference. Up to 64KB of memory can be exposed per request.

The exposed memory is in the OpenSSL service process area and can contain secret keys used for X.509 certificates, user names, passwords, web cookies, and even the contents of user communications.

RECOMMENDATIONS

- Update vulnerable servers or mitigate the risk AND replace the public/private keys and SSL/TLS certificate associated with the servers. Revoke the earlier (potentially compromised) SSL/TLS certificate(s). Understand that, although absolutely necessary, revocation isn't 100% effective because of shortfalls in client use of revocation [7]. Make sure your certificate authority is not vulnerable before obtaining new certificates.
- Evaluate the risks (described below) and evaluate other steps such as expiring passwords, notifying users, monitoring account access, etc.
- Use this opportunity to evaluate improving the configuration, cipher (e.g. TLS 1.2), and capabilities (e.g. Perfect Forward Secrecy) of your SSL/TLS services [2], [3], [4], [5], [6].
- Provide information and guidance for your users.
- Warn your users about the inevitable phishing to steal user account information by spoofing password change notifications.
- If you have questions or seek assistance, contact the REN-ISAC at soc@ren-isac.net.

Is My Enterprise Affected?

Unquestionably yes. Either directly (services that you operate and provide) or indirectly (services provided to you by other parties). Most likely both.

What Are The Vulnerable Services?

This list is not comprehensive. Vulnerable services may include:

- Secure web (https).
- Network systems including those that allow only administrator access, e.g. routers, and those that provide user-authenticated services, e.g. VPN servers.
- Applications and appliances that employ secure remote connections.

What's At Risk?

1. Your capability to deliver secure web services. Compromise of the secret keys associated to X.509 certificates used by the web server would allow an attacker to intercept and decrypt all traffic and/or impersonate the server.
2. User names and passwords used to access vulnerable servers.
3. Session keys and cookies used in sessions with vulnerable servers.
4. Content of communications that occurred over vulnerable servers.
5. Other information exposed in the memory leak that could allow an attacker to mount additional attacks against the server (likely becomes irrelevant when you upgrade OpenSSL).

It's IMPORTANT to note that risk to your enterprise not only involves internal services but includes use of services provided by other parties, e.g. financial, cloud, federated authentication, etc.

Is This Vulnerability Currently Being Exploited?

Yes. It's very easy to exploit. Tools and how-to information are easily obtained. Universities have reported observing exploitation attempts (see Can I Detect Attacks? below).

How Can I Tell If I've Been Compromised?

If you've already been compromised you probably won't be able to tell. Exploitation of the vulnerability leaves no log information on the affected server. Your first indication may be in seeing stolen credentials used in follow-on attacks.

Can I Detect Attacks?

Yes. There are signatures available for intrusion detection systems.

For open-source IDS (Snort, Suricata, Bro):

http://blog.fox-it.com/2014/04/08/openssl-heartbleed-bug-live-blog/
http://blog.inliniac.net/2014/04/08/detecting-openssl-heartbleed-with-suricata/
http://blog.bro.org/2014/04/detecting-heartbleed-bug-using-bro.html

For commercial IDS, refer to your vendor.

Should I Be Resetting All My Users' Passwords?

Evaluate the risk and trade-offs. Are you able to determine if passwords were handled by a vulnerable server? Do you require periodic password changes thwarting the use of organizational passwords at external web properties? Do you require two-factor authentication for business functions?

In the absence of having information about what data might have been exposed, the most conservative response would be to reset all user credentials. Don't count on users voluntarily resetting their passwords. Implement an expiration process. Conduct the process in stages, e.g. resetting privileged/sensitive accounts immediately, before addressing all other accounts in staged waves. In many cases, password change processes and support personnel will not be scaled to support 100% required changes all at once.

Notify all users of the broader issue concerning services provided outside your enterprise. Mandate changes for users of vulnerable external business functions and suggest that users consider their active personal accounts as well. However, don't change passwords on external services until you know their vulnerabilities have been addressed.

Many people may not know their password(s), having lost them to the "remember password" function in popular web browsers. How does your organization support users changing or reinstating passwords if they don't know their current password? Trivia questions? Personal appearance with picture id in-hand?

End users will be very confused and need lots of support. Supporting information on web pages will help users and relieve the burden on help desk and support personnel. Prepare your help desk for the onslaught.

It's an excellent time to reinforce the best practice of unique passwords for every account and password wallets to manage the passwords. Also, if you're not already doing so, to evaluate using two-factor authentication for business functions.

Do I Need To Consider This A Breach For Notification Purposes?

Evaluate whether to notify users of affected systems to change their passwords (see Should I Be Resetting All My User's Passwords?).

Concerning a more broad notification of breach, this will be very hard to determine. Evidence for and determination of the extent of a successful attack will be indirect, e.g. compromised accounts used by criminals, subsequent man-in-the-middle attacks on secure web traffic, or compromised super user accounts being used from odd locations.

Notification concerning a "potential breach" needs to be guided by local policy and law.

What Systems Are Vulnerable?

System vulnerability and patch information is quickly evolving. Track at the CERT and SANS web pages:

http://www.kb.cert.org/vuls/id/720951
https://isc.sans.edu/forums/diary/Heartbleed+vendor+notifications/17929

Can I Test For Vulnerable Systems?

Various tests are available:

http://seclists.org/nmap-dev/2014/q2/att-27/ssl-heartbleed.nse
https://github.com/rapid7/metasploit-framework/blob/master/modules/auxiliary/scanner/ssl/openssl_heartbleed.rb
http://www.tenable.com/plugins/index.php?view=single&id=73412

Online tests (use at your own risk - you potentially identify vulnerable servers to unknown persons)

https://community.qualys.com/blogs/securitylabs/2014/04/08/ssl-labs-test-for-the-heartbleed-attack
http://filippo.io/Heartbleed/
http://possible.lv/tools/hb/

Other Notes

SSH is not vulnerable to this issue as far as we know at this time.

References

[1] http://www.ren-isac.net
[2] http://en.wikipedia.org/wiki/Transport_Layer_Security
[3] https://www.ssllabs.com/ssltest/
[4] http://en.wikipedia.org/wiki/Forward_secrecy
[5] https://owasp.org/index.php/Transport_Layer_Protection_Cheat_Sheet
[6] https://www.eff.org/deeplinks/2014/04/why-web-needs-perfect-forward-secrecy

[7] http://www.darkreading.com/endpoint/authentication/solving-the-ssl-certificate-revocation-checking-shortfall/d/d-id/1137268
[8] http://www.ren-isac.net/about/advisory.html#technical
[9] http://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-initiative/about

Credits

Thanks to the REN-ISAC Technical Advisory Group [8] and members of the HEISC [9] for assistance in assembling this notification, and to REN-ISAC members for valuable shared information.

Copy of this Alert is available on the REN-ISAC web site at:
http://www.ren-isac.net/alerts/REN-ISAC_Alert_HeartBleed_20140410.html

We'd appreciate your input on additional means to protect from the threat and general feedback concerning this Alert. If you have any questions, please don't hesitate to e-mail us at soc@ren-isac.net.

Sincerely,

Your REN-ISAC Team
http://www.ren-isac.net
24x7 Watch Desk +1(317)278-6630

-o0o-