The Heartbleed Bug

Deprecated

Note that this page has been deprecated. The information it contains is no longer current.

This wiki page is a work in progress and will be updated as new information is received and processed.

The Heartbleed Bug

A serious vulnerability has been found to affect many Internet hosts. The Heartbleed Bug, announced publicly on April 7, 2014, affects certain versions of OpenSSL in circulation since 2012.

The following InCommon servers were **not** running a vulnerable version of OpenSSL and therefore were **not** affected by this bug:

- Federation Manager (service1.internet2.edu)
- Metadata Services (wayf.incommonfederation.org, md.incommon.org)
- Discovery Service (wayf.incommonfederation.org)
- Error Handling Service (ds.incommon.org)

The following InCommon server, which serves a single HTML resource, was found to be running a vulnerable version of OpenSSL:

- ops.incommon.org

The above server was patched, its TLS certificate was revoked, and a new TLS key and certificate were installed. The content on that server was reviewed and found to be intact. These steps restored the integrity of the HTML resource.

Recommendations for Deployers

If your SAML deployment relies on an affected version of OpenSSL, you should take the following actions to mitigate that vulnerability:

1. Patch the affected version of OpenSSL
    a. Follow the OS vendor's instructions to upgrade OpenSSL to the latest version
2. Revoke your browser-facing TLS certificate
    a. Configure the system with a new trusted TLS key and certificate
3. Revoke your SAML certificate in metadata
    a. Migrate a new certificate into metadata

When all but step 3 above have been completed, follow these additional steps to *migrate a new certificate into metadata*:

1. Read the X.509 Certificates in Metadata wiki page
    a. Use a long-lived, self-signed certificate
2. IdP operators: Read the IdP Key Handling wiki page (SP owners might also benefit from reading this page)
    a. Handle the private IdP signing key securely!
3. Read the Certificate Migration wiki page and its child pages
    a. Unless there is evidence that your IdP signing key has been compromised, *migrate a new certificate into metadata*, do not simply replace the old certificate (which will adversely affect interoperability).
    b. Assuming your SP partners follow InCommon recommendations with respect to Metadata Consumption, wait at least 24 hours for newly updated metadata to propagate throughout the Federation.

Note Well!

To the extent that you believe your system is vulnerable to The Heartbleed Bug, we provide the above noted guidance. Due to the unique nature of each affected system, you are of course the best source for determining solutions that meet the needs of a given system.

To ensure that you are receiving metadata updates from partners in a timely manner, review the metadata refresh process of each of your SAML deployments *regardless of whether or not it is vulnerable*:

- Is your software pointing to the correct metadata aggregate? See: Metadata Aggregates
- Have you installed the new metadata signing certificate? See: Metadata Signing Certificate
- Is your metadata refresh process optimally configured? See: Metadata Client Software

If you recently completed the widely publicized Metadata Migration Process, the above issues will have been already addressed.

Implementation-specific Information

If you deploy the Shibboleth SP on Windows, versions 2.5.0 (or later), consult the Shibboleth Security Advisory issued on 9 April 2014.

If you are using simpleSAMLphp, we recommend reading the entire thread entitled "heartbleed and SimpleSAMLphp (https://groups.google.com/forum/#\!topic/simplesamlphp/XphXXmVhMVI)" on the simpleSAMLphp mailing list.

Lessons Learned

For further discussion:

- The benefits of federated login at the SP (no shared secrets)
- The security and convenience of multilateral federation
- The agility of a metadata-based trust model
- The importance of secure, automated metadata refresh
- The advantages and disadvantages of deploying a web server (e.g., Apache) in front of the IdP
- The advantages and disadvantages of enabling "forward secrecy" on a web server
- Is there value in defining separate keys for back-channel TLS?

> *The Internet is unfortunately not as safe and reliable as many people, even among IT experts, tend to believe, and only a joint effort can fix it. (Lessons learned from the Heartbleed incident by Alexei Balaganski)*

Resources

- The Heartbleed Bug
- For more information, contact: admin@incommon.org