ergon hgi SysSec pallas secunet

nrw-unITS IT-Sicherheit Nordrhein-Westfalen

Arbeitsgruppe Websicherheit

Heartbleed Bug - Was ist zu tun?

Was bedeutet die OpenSSL Sicherheitslücke „Heartbleed" für die Anbieter und Nutzer von Webdiensten? Was ist zu tun um Schäden zu vermeiden oder zu reduzieren? Wie kann man sich zukünftig gegen ähnliche Risiken wappnen?

Einleitung

Die OpenSSL Sicherheitslücke Heartbleed kursiert aktuell in allen Medien, meist verbunden mit Klassifizierungen wie „Super GAU" oder „Katastrophe". Dieses Whitepaper soll Anbieter und Nutzer von Web-Portalen und vergleichbaren Diensten über die wichtigsten fachlichen Details informieren.

Die Autoren verbinden mit den im Folgenden dargestellten Informationen ausdrücklich keinerlei Wertung: Fehler, insbesondere Software-Fehler, lassen sich nicht vollständig vermeiden. Die daher unvermeidlichen Risiken durch Sicherheitslücken und Schwachstellen können im Vorfeld allenfalls durch allgemeine Vorsorgemaßnahmen und eine robuste IT-Sicherheitsarchitektur gemindert werden. Beim Bekanntwerden von Sicherheitslücken ist dann schnell und zielgerichtet zu handeln.

Was ist passiert?

Es wurde eine Sicherheitslücke in der Softwarekomponente OpenSSL bekannt. Diese betrifft die Versionen „1.0.1" bis „1.0.1f" von OpenSSL mit aktiviertem Heartbeat-Mechanismus. Der Fehler existiert bereits seit ca. 2 Jahren. OpenSSL wird vielfach als Modul eingesetzt, um das TLS-Protokoll (früher: SSL-Protokoll) zu realisieren. Das TLS-Protokoll dient zum Aufbau von authentisierten und verschlüsselten Netzwerkverbindungen. Andere Software, welche OpenSSL beinhaltet oder verwendet, kann ebenfalls betroffen sein. Hierfür werden typischerweise andere Versions-Schemata verwendet. Die Angabe ob eine Software verwundbar ist oder nicht kann beim Hersteller eingeholt werden.

Die betroffenen Versionen werden von sehr vielen Diensten im Internet eingesetzt - es können alle Dienste und Lösungen betroffen sein, die TLS verwenden (neben Webdiensten über HTTPS z.B. auch SSL-VPN, OpenVPN, E-Mail-Verbindungen über IMAPs und VoIP über SIPs). Auch diverse Client-Anwendungen sind betroffen (z.B. wget 1.15). Im Gegensatz zu Servern muss der Client jedoch aktiv die Verbindung mit einem bösartigen Server aufbauen, bevor dieser die Sicherheitslücke ausnutzen kann.

Die Sicherheitslücke ermöglicht Angreifern, auf Speicherinhalte des OpenSSL verwendenden Prozesses zuzugreifen. Diese Speicherinhalte können unterschiedliche Daten beinhalten, z.B. private Schlüssel des verwendeten Zertifikats oder Anmeldedaten von Benutzern (z.B. Benutzername, Passwort). Falls der private Schlüssel entwendet wurde, so kann ein Angreifer das entwendete SSL-Zertifikat beliebig nutzen, also z.B. TLS-Verbindungen für den angegriffenen Webdienst übernehmen (Phishing, Man-in-the-Middle Angriff) und unter bestimmten Umständen (z.B. falls kein Perfect Forward Secrecy verwendet wurde) sogar früher aufgezeichneten TLS-Verkehr entschlüsseln. Darüber hinaus kann der Angreifer andere ausgespähte Daten beliebig nutzen, also z.B. Benutzerdaten für die Anmeldung verwenden.

Die Sicherheitslücke betrifft sowohl die Server-Seite als auch die Client-Seite und kann real durch Angreifer ausgenutzt werden, wie erfolgreiche Angriffsversuche zeigten. Ob die Sicherheitslücke tatsächlich ausgenutzt wurde lässt sich im Nachhinein nicht zuverlässig ermitteln. Es muss jedoch zur Planung der weiteren Maßnahmen davon ausgegangen werden, dass die Zertifikate und Benutzerdaten kompromittiert wurden.

Was ist akut zu tun?

Web-Dienstleister

Der Begriff „Webdienste" umfasst im Folgenden nicht nur die allgemein im Internet zugänglichen Websites und Portale, sondern auch Angebote für bestimmte Benutzergruppen (Kundenportale, Partnerportale, Mitarbeiterportale, Intranets) und sonstige Services, die SSL/TLS nutzen, z.B. VPN, E-Mail, SSH.

Sofern OpenSSL oder eine andere Software in einer verwundbaren Version genutzt wird, sind im Überblick folgende Maßnahmen durchzuführen:

- Aufgrund der Tragweite eines Angriffs raten wir dringend davon ab, die Schwachstelle zu ignorieren. Falls die im Folgenden aufgeführten Maßnahmen für ein spezielles System nicht anwendbar sein sollten, ist auch die vorübergehende Deaktivierung des Dienstes in Erwägung zu ziehen, um weiteren Schaden zu vermeiden.

- OpenSSL mit einer Version mindestens „1.0.1g“ (bzw. der vom Anbieter/Hersteller als Patch bereitgestellten Version) aktualisieren.
- Sofern kein Patch verfügbar ist, prüfen, ob die Heartbeat-Extension deaktiviert werden kann. Alternativ könnte ein nicht betroffenes Produkt eingesetzt werden.
- Prüfen, welche Zertifikate und sonstige vertrauliche Daten kompromittiert sein könnten. Alle Zertifikate und alle Daten die im Zusammenhang mit OpenSSL-Sessions auf einem verwundbaren System genutzt wurden, sind dabei als potenziell kompromittiert anzusehen
- Sofern ein Zertifikat potenziell kompromittiert ist, betrifft dies tatsächlich den Private-Key (privaten Schlüssel), auf dem das Zertifikat basiert. Für den Austausch ist ein neuer Private-Key zu generieren und darauf basierend ein neues Zertifikat zu erstellen und zu installieren. Nach erfolgreicher Installation ist das potenziell kompromittierte Zertifikat zu widerrufen (revozieren).
- Sofern weitere Daten potenziell kompromittiert sind (z.B. Anmeldedaten) sollten die Benutzer nach Schließen der Sicherheitslücke und Austausch der Zertifikate über den Status und die empfohlenen Maßnahmen informiert werden (z.B. Wechsel des Passworts). Das Auffordern der Nutzer zum Passwortwechsel beim nächsten Anmelden ist ernsthaft zu erwägen.

Web-Nutzer

Es kursieren Listen der betroffenen Webseiten im Internet. Es ist dabei allerdings zu beachten, dass auch Dienste, die aktuell als sicher eingestuft sind, womöglich zeitweise betroffen waren. Auf Nummer sicher gehen Web-Nutzer bei der Planung der Maßnahmen, wenn sie davon ausgehen, dass alle durch sie genutzten Webdienste kompromittiert waren und evtl. noch sind. Bereits ein kompromittiertes E-Mail-Konto ermöglicht einem Angreifer möglicherweise, die Passwörter für andere Dienste auszutauschen. Soweit gleiche oder ähnliche Passwörter für mehrere Dienste im Internet genutzt werden (wovon generell abzuraten ist!), sind auch diese Dienste gefährdet.

Im Überblick sollten Web-Nutzer folgende Maßnahmen ergreifen:

- Potentiell betroffene Webdienste sollten auf keinen Fall genutzt werden, sofern vertrauliche Daten transferiert werden. Dazu gehören insbesondere alle Dienste, die eine Benutzeranmeldung erfordern. Die Gefährdung durch einen Webdienst ist erst dann behoben, wenn die Sicherheitslücke geschlossen und das Zertifikat ausgetauscht wurden.
- Es sind alle genutzten Webdienste aufzulisten, die SSL/TLS (https) verwenden und über die vertrauliche Daten (insbesondere Anmeldedaten) ausgetauscht werden. Insbesondere aufzulisten sind E-Mail-Konten, Web-Shops, Social-Media (z.B. Facebook), Online-Banking, Web-Foren.
- Für jeden aufgelisteten Webdienst ist zu prüfen, ob er aktuell (noch) betroffen ist (z.B. per https://www.ssllabs.com/ssltest/). Weitere Maßnahmen sind erst sinnvoll, wenn ein Webdienst nicht (mehr) betroffen ist.
- Für die wichtigsten, aber insbesondere die betroffenen Webdienste sind die Passwörter zu ändern. Dies ist eine sehr gute Gelegenheit, einen umfassenden Passwortwechsel für alle Web-Konten durchzuführen, etwas das sowieso regelmäßig getan werden sollte. Hierbei sollten hinreichend komplexe und lange Passwörter gewählt werden, die sich von Dienst zu Dienst unterscheiden.

Was ist noch zu tun und zu beachten?

Web-Dienstleister

Sofern OpenSSL mit einer nicht betroffenen Version vor „1.0.1" genutzt wird, ist bei einem Update darauf zu achten, dass ausschließlich auf eine Version aktualisiert wird, die vom Anbieter/Hersteller als ebenfalls nicht betroffen oder gefixt deklariert ist.

Sofern für die Authentisierung der Gegenstelle ebenfalls Zertifikate verwendet werden (Client-Zertifikate) wird für wichtige Dienste empfohlen, diese ebenfalls auszutauschen - sofern nicht sichergestellt werden kann, dass die Gegenstelle zu keiner Zeit verwundbar war. Ein Angreifer im Besitz des geheimen Schlüssels des Client-Zertifikats hätte sonst eventuell die Möglichkeit, sich als regulärer Benutzer zu authentisieren. Die gängigen Browser Firefox, Safari, Internet Explorer, Opera und Chrome sind und waren allerdings nicht verwundbar – sie verwenden andere TLS-Implementationen. Java Clients sind ebenfalls nicht betroffen – auch sie bringen eine eigene TLS-Implementation mit.

Web-Nutzer

Web-Nutzer sollten regelmäßig ihre Konten auf Unregelmäßigkeiten und aussergewöhnliche Transaktionen prüfen. Ebenfalls anzuraten ist ein regelmäßiger Austausch der Passwörter. Dies muss vielleicht nicht monatlich erfolgen, einmal pro Jahr ist aber das Minimum (je nach gewählter Komplexität und Länge des Passwortes und abhängig von der Wichtigkeit des Dienstes). Bei verschlüsselten Webseiten sollte man prüfen, ob das vom Server verwendete Zertifikat nach dem 7. April 2014 ausgestellt wurde. Bei wichtigen Diensten sollte darüber hinaus geprüft werden, ob der Anbieter des Dienstes das alte, möglicherweise kompromittierte Zertifikat gesperrt hat und diese Sperrung auch von der verwendeten Clientsoftware (z.B. Browser) erkannt wird. Ansonsten könnte ein Angreifer, der über das kompromittierte Zertifikat und den privaten Schlüssel verfügt, weiterhin erfolgreich Angriffe durchführen (z.B. Phishing, Man-in-the-Middle).

Was kann gegen zukünftige Heartbleeds getan werden?

Schwachstellen werden immer wieder auftreten - manche werden früher veröffentlicht, manche später und einige werden gar nicht öffentlich bekannt. Niemand weiß im Voraus, wo sie auftreten und

wie sie sich auswirken. Daher kann es auch keine spezifischen Maßnahmen zur Vorbeugung geben. Das allgemeine Risiko hinsichtlich möglicherweise auftretender Schwachstellen kann jedoch reduziert werden, indem man sich nicht nur auf einen einzelnen Sicherheitsmechanismus verlässt. Vielmehr sind Anordnung und Stärke der Schutzmaßnahmen am Einsatzzweck und der Höhe des potenziellen Schadens auszurichten.

In jedem Fall ist kontinuierliche Aufmerksamkeit gefordert, um hinreichend schnell reagieren zu können sobald weitere kritische Sicherheitslücken offenbar werden. Dies beinhaltet nicht zuletzt, die Herstellerinformationen zu Updates und Schwachstellen zu beachten und Patches zeitnah zu installieren.

Web-Dienstleister

Als allgemeine Sicherheitsmaßnahme wird empfohlen, Webdienste in mehrere Sicherheitszonen zu separieren. Dieses Vorgehen bewirkt, dass eine auftretende Schwachstelle mit sehr hoher Wahrscheinlichkeit nicht sofort auch eine Sicherheitslücke darstellt, da weitere Sicherheitsmaßnahmen eine Ausnutzung verhindern. Eine weitere Strategie mit ähnlicher Wirkung ist der Einsatz mehrerer komplementärer Schutzmechanismen.

Als Best Practice haben sich folgende Massnahmen etabliert: Zwei-Faktor Authentisierung, Einsatz einer Web Application Firewall, SSL Terminierung auf dem Gateway, Filterung der Daten, Perfect Forward Secrecy, Transaktionssignierung, Client Fingerprinting zur Erkennung von entführten Sessions und generische Schutzmassnahmen wie Cookie-Schutz und URL-Signierung oder -Verschlüsselung.

Web-Nutzer

Damit ein einzelner kompromittierter Webdienst andere genutzte Webdienste nicht ebenfalls kompromittiert, wird dringend empfohlen, für jeden unabhängigen Webdienst verschiedene Anmeldedaten (mindestens unabhängige Passwörter) zu verwenden. Für besonders schützenswerte Daten ist der Nutzen eines Webdienstes gegen das immer vorhandene Risiko abzuwägen. Die beste Möglichkeit vertrauliche Daten zu schützen, ist, diese gar nicht erst ins Web zu transferieren!

Arbeitsgruppe Websicherheit

Sicher Surfen, Schutz der eigenen Webseiten
Die Arbeitsgruppe Websicherheit hat sich das Ziel gesetzt, praktische Informationen zum Schutz von Web-Server-Infrastrukturen und Web-Clients bereitzustellen. Diese Informationen sollen Ihnen nicht nur einen Überblick über die aktuelle Bedrohungssituation verschaffen, sondern Sie bei der Selbst-einschätzung Ihres Unternehmens unterstützen und ganz konkret die wichtigsten Schritte und Schutzmaßnahmen darstellen.

Autorenteam

Autor:

Dr. Martin Burkhart
Product Manager Web Application Security
martin.burkhart@ergon.ch

Unternehmen:

Ergon Informatik AG
www.ergon.de

Autor:

Prof. Dr. Thorsten Holz
Lehrstuhl für Systemsicherheit
thorsten.holz@rub.de

Unternehmen:

Ruhr-Universität Bochum
www.syssec.rub.de

Autor:

Stephan Sachweh
Geschäftsführer
stephan.sachweh@pallas.com

Unternehmen:

Pallas GmbH
www.pallas.com

Autor:

Dr. Markus Müller
Bereichsleiter Managed Security Services
markus.mueller@secunet.com

Dirk Reimers
Bereichsleiter PenTest & Forensik
dirk.reimers@secunet.com

Alexander Schlensog
Bereichsleiter Sicherheitsmanagement
alexander.schlensog@secunet.com

Unternehmen:

secunet Security Networks AG
www.secunet.com