

Heartbleed-Bug

09.04.2014 15:08

Heartbleed-Bug - was ist das?

Der Heartbleed-Bug nutzt einen Fehler in der sogenannten "Heartbeat"-Funktion von OpenSSL. Dies ist eine Kommunikations-Funktion, die Statusinformationen zwischen zwei Partnern austauscht, v. a. um festzustellen, ob die Gegenstelle noch aktiv ist. Eine fehlende Implementierung eines Speicherzugriffs kann dazu führen, dass ein Angreifer bis zu 64 KB aus dem Arbeitsspeicher des Gegenübers auslesen kann, z. B. Usernamen, Passwörter, Session-Daten oder verschlüsselte E-Mails, die als Klartext lesbar werden.

Wer ist betroffen?

Grundsätzlich betrifft der Fehler jeden Dienst, der OpenSSL in der Version 1.0.1 bis 1.0.1f oder OpenSSL 1.0.2-beta verwendet. Dies sind vor allem Webserver, aber auch Server, die z. B. für Dienste wie E-Mail, VPN, Plesk oder Adminpanels genutzt werden. Verwundbar sind die Distributionen RHEL6 / CentOS6, Debian 7 und FreeBSD 10.

Nicht betroffen sind Distributionen, die auf der älteren OpenSSL 0.9.8 aufbauen. Nutzer des Apple-Betriebssystems Mac OS X Mavericks zum Beispiel sind wegen der älteren OpenSSL-Versionen nach aktuellem Kenntnisstand vor den Angriffen sicher.

Was ist zu tun?

Updates und Patches einspielen

Jedes System mit einer angreifbaren Version von OpenSSL benötigt einen Patch oder ein Update. Für die Distributionen RHEL6 / CentOS6, Debian 7 und FreeBSD 10 sind Aktualisierungen verfügbar, die die Lücke schließen. Selbst übersetzte Versionen von OpenSSL mit der Option `-DOPENSSL_NO_HEARTBEATS` sind nicht betroffen, die Quellen ab 1.0.1g enthalten einen Fix. Distributionsbezogene Updates können wie folgt eingepflegt werden:

- CentOS/RHEL: `yum -y update openssl`
- Debian `apt-get update; apt-get -y install openssl libssl1.0.0`

Wichtig: Nach Installation der Updates ist es unbedingt erforderlich, sämtliche Dienste des Servers neu zu starten oder das System direkt zu rebooten.

SSL-Zertifikate erneuern (Reissue)

Für alle SSL-Zertifikate, die über den SSL Manager 2.0 von InterNetX geordert wurden,

kann **KOSTENLOS** ein Reissue durchgeführt werden. **Unternehmens-validierte Zertifikate** (alle außer Thawte SSL 123) werden ohne weitere Prüfung oder Verifikation ausgestellt.

SSL-Zertifikate löschen (Revoke)

Aktuell verifizieren die Anbieter Symantec, Thawte und GeoTrust die Daten. Alle neu ausgestellten Zertifikate werden automatisch gelöscht, als Termin dafür ist der letzte Arbeitstag der folgenden Woche anvisiert.