Heartbleed bug find triggers OpenSSL security advisory

April 8 2014, by Nancy Owano

A flaw called Heartbleed in OpenSSL, which is a software library used for the protection and security of millions of websites, was uncovered by Neel Mehta of Google Security, who first reported it to the OpenSSL team, triggering Monday's release of a fix for the bug along with a security advisory. Dated Monday, the OpenSSL security advisory said the flaw involved "a missing bounds check in the handling of the TLS [Transport Layer Security] heartbeat extension," which could be used to reveal "up to 64k of memory to a connected client or server." The advisory said this issue did not affect versions of OpenSSL prior to 1.0.1. Namely, what was affected were 1.0.1f, 1.0.1e, 1.0.1d, 1.0.1c, 1.0.1b, 1.0.1a, 1.0.1. The bug was fixed in OpenSSL 1.0.1g. "Affected users should upgrade to OpenSSL 1.0.1g. Users unable to immediately upgrade can alternatively recompile OpenSSL with -DOPENSSL_NO_HEARTBEATS." In the notice Mehta of Google

Security was thanked for discovering the bug and Adam Langley and Bodo Moeller were thanked for preparing the fix.

Meantime, a team of security engineers at security company Codenomicon independently explored the bug, which their team found while improving the SafeGuard feature in its security testing tools; they reported the bug to the NCSC-FI for vulnerability coordination and reporting to OpenSSL team. Codenomicon issued a fully detailed page examining Heartbleed and its vulnerabilities:"The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users."

Codenomicon is headquartered in Oulu, Finland and California with offices in Singapore and Hong Kong. The company's testers utilized an attacker's perspective and attacked the company from outside, "without leaving a trace." The Codenomicon team said they did not use any credentials or privileged information and yet were able to steal "secret keys used for our X.509 certificates, user names and passwords, instant messages, emails and business critical documents and communication."

According to Codenomicon, the bug was introduced to OpenSSL in December 2011 and "the OpenSSL 1.0.1g released Monday fixes the bug." OpenSSL is used to protect sensitive data as it travels back and forth, said BBC News. *Ars Technica* called it "the world's most popular code library for implementing HTTPS encryption in websites, e-mail servers, and applications."

The bug itself is called "Heartbleed" because it occurs in the heartbeat extension. Codenomicon explained that the bug is in the OpenSSL's

implementation of the TLS/DTLS (transport layer security protocols) heartbeat extension (RFC6520). "When it is exploited it leads to the leak of memory contents from the server to the client and from the client to the server."

According to BBC News, full protection might require "updating to the safer version of OpenSSL as well as getting new security certificates and generating new encryption keys." Similarly, Jeremy Kirk of the IDG News Service said administrators were advised to apply the up-to-date version of SSL, revoke any compromised keys and reissue new keys.

Posing the question, "Is there a bright side to all this?" Codenomicon commented that for service providers affected, "this is a good opportunity to upgrade security strength of the secret keys used."

Citation: Heartbleed bug find triggers OpenSSL security advisory (2014, April 8) retrieved 26 April 2024 from https://techxplore.com/news/2014-04-heartbleed-bug-triggers-openssl-advisory.html