DARC

DenyAll Research Center

Security Research Advisory – December 14th, 2017

ROBOT attack

What happened?

The Bleichenbacher attack is back, now named "Return Of Bleichenbacher's Oracle Threat" (ROBOT). This 19-year-old vulnerability can allow an attacker to decrypt HTTPS traffic by exploiting some RSA encryption implementations.

ROBOT is a variation of the old Bleichenbacher attack from 1998 which is a padding oracle attack on RSA PKCS#1 v1.5 encryption for key exchange.

Hosts that are supporting RSA encryption with one of the vulnerable TLS/SSL implementations can be impacted.

Sources: https://robotattack.org/, http://archiv.infsec.ethz.ch/education/fs08/secsem/bleichenbacher98.pdf

Detail of the vulnerability

The Bleichenbacher attack is applicable to the TLS-RSA key exchange. This key exchange is used in all cipher suites having names starting with TLS_RSA (e.g. TLS_RSA_WITH_AES_128_CBC_SHA256).

An attacker can make use of specially crafted TLS client handshakes (different RSA PKCS#1 v1.5 paddings, valid or not) with the TLS server acting as an oracle (based on the response status) to decrypt arbitrary ciphertext without access to the private key (i.e. adaptive chosen-ciphertext attack).

The novelty of the ROBOT attack, compared to the original Bleichenbacher's one, is that TLS implementations known to be vulnerable may return different TLS alerts and/or connection closures depending on the crafted padding, and this side-channel information can be used to improve the efficiency of the attack (less requests needed).

DenyAll Statement

The DenyAll products are *not* vulnerable to this attack.

The OpenSSL's implementation of TLS used in DenyAll products always completes invalid handshakes before returning the (same) appropriate TLS-alert, and so according to the TLS 1.0 (and later) specification's recommendation against this old and well known attack. In this regard, the new attack doesn't exploit a new TLS vulnerabilty, servers immune to the old Bleichenbacher attack remain immune to this new attack, while vulnerable servers may now face a faster attack.

About the DARC

The Deny All Research Center (DARC) is an internal division of Deny All, which focuses on threat analysis and mitigation. Over the last 10 years, this department's research has contributed to the design of state-of-the art Web application security solutions. More information on DenyAll can be found at www.denyall.com