Silver Peak Security Advisory

Notification

Return Of Bleichenbacher's Oracle Threat (ROBOT Attack) – A TLS Vulnerability

TLS implementations may disclose side channel information via discrepancies between valid and invalid PKCS#1 padding

VU#144389 originally published by CERT on December 12, 2017

CVE IDs:CVE-2017-6168 CVE-2017-1000385 CVE-2017-17427 CVE-2017-13098 CVE-2017-13099 CVE-2017-17428 CVE-2017-17382 CVE-2012-5081 CVE-2016-6883

Summary:

This is a TLS security advisory for VU#144389.

ROBOT is the return of a 19-year-old vulnerability that allows performing RSA decryption and signing operations with the private key of a TLS server.

ROBOT only affects TLS cipher modes that use RSA encryption. Most modern TLS connections use an Elliptic Curve Diffie Hellman key exchange and need RSA only for signatures. We believe RSA encryption modes are so risky that the only safe course of action is to disable them. Apart from being risky these modes also lack forward secrecy.
By disabling RSA encryption we mean all ciphers that start with TLS_RSA. It does not include the ciphers that use RSA signatures and include DHE or ECDHE in their name. These ciphers are not affected by our attack.

We carefully reviewed all Silver Peak products that support TLS and have determined that this attack is not applicable to us.

Applicability to Silver Peak deployments: None

Silver Peak VXOA release for NX/VX/VRX/CPX/EdgeConnect appliances is NOT susceptible to this vulnerability.

Silver Peak Unit Orchestrator/Cloud Orchestrator/GMS is NOT susceptible to this vulnerability.

Silver Peak Cloud Portal is NOT susceptible to this vulnerability.

Recommended Action for Silver Peak Customers:

No action required

Resolution:

N.A.

Details:

The full details of the advisory are located at-

https://robotattack.org/
https://www.kb.cert.org/vuls/id/144389

Thank you.

Security Incident Response Team

Silver Peak