Silver Peak Security Advisory

Notification

"The Dangers of Key Reuse: Practical Attacks on IPsec IKE" published on August 15, 2018

Summary:

This is a security advisory for the issues described at the Usenix Security Symposium in the paper entitled "The Dangers of Key Reuse: Practical attacks on IPsec IKE" as published in https://www.ei.rub.de/media/nds/veroeffentlichungen/2018/08/13/sec18-felsch.pdf

Related CVE IDs for the same issues from other vendors are: CVE-2018-0131, CVE-2017-17305, CVE2018-8753, and CVE-2018-9129

In this paper, Dennis Felsch, Martin Grothe and team show that reusing a key pair across different versions and modes of IKE can lead to cross protocol authentication bypasses, enabling the impersonation of a victim host or network by attackers. They exploit a Bleichenbacher oracle in an IKEv1 mode, where RSA encrypted nonces are used for authentication. Using this exploit, they break these RSA encryption based modes, and in addition break RSA signature based authentication in both IKEv1 and IKEv2. Additionally, they describe an offline dictionary attack against the PSK (Pre-Shared Key) based IKE modes, thus covering all available authentication mechanisms of IKE.

Bu default, Silver Peak does not use IKE-based authentication in VXOA releases 8.1.6 and later hence this vulnerability is not applicable to the bulk of Silver Peak deployments. Optionally, Silver Peak supports IKE-based IPsec, when configured, and by default in VXOA releases prior to 8.1.6. Even when configured for IKE-based IPsec, Silver Peak is not vulnerable as RSA based authentication is not supported by Silver Peak. The paper also describes an additional issue with dictionary attacks on pre-shared keys. Silver Peak's pre-shared keys exceed the password requirements as specified by the NIST security standard of FIPS 140-2 level 2. This greatly lowers the probability of a dictionary or a brute force attack on pre-shared keys. The overall applicability to Silver Peak deployments of this vulnerability is low to none.

Applicability to Silver Peak Deployments: Low to None

Silver Peak VXOA releases for NX/CPX/EdgeConnect appliances (both physical, virtual, cloud) are NOT susceptible to this vulnerability.

This vulnerability is not applicable to

Silver Peak Cloud Services - Cloud Orchestrator, Orchestrator^{SP} and Cloud Portal

Silver Peak Orchestrator

Recommended Action for Silver Peak Customers:

None

Resolution:

None

References:

The full details of the advisory and the vulnerabilities are found at-

https://www.ei.rub.de/media/nds/veroeffentlichungen/2018/08/13/sec18-felsch.pdf
https://web-in-security.blogspot.com/2018/08/practical-bleichenbacher-attacks-on-ipsec-ike.html
https://web-in-security.blogspot.com/2018/08/practical-dictionary-attack-on-ipsec-ike.html

Thank you.

Product Security Incident Response Team

Silver Peak