Array Networks Security Advisory:
TLS ROBOT Vulnerability (CWE-203)

Advisory Date: January 2, 2018

Overview

TLS implementations that do not strictly follow the descriptions in RFC 5246 may leak information to an attacker when they handle PKCS #1 v1.5 padding errors in ways that let the attacker distinguish between valid and invalid messages. An attacker may exploit discrepancies between TLS error messages returned by the SSL server to obtain the pre-master secret key used to decrypt sensitive data when the SSL server is running a vulnerable TLS implementation and enables RSA cipher suites. This vulnerability is referred to as Return of Bleichenbacher's Oracle Threat (ROBOT) vulnerability.

Reference: CWE-203 http://www.kb.cert.org/vuls/id/144389

Impact

Array APV and AG Series products installed with SSL hardware cards, as well as vAPV and vxAG virtual appliances that use SSL hardware cards installed on virtualization platforms/hypervisors (such as Array's AVX Series network functions platforms and others), are vulnerable to this attack. When TLS utilizing RSA cipher suites is enabled on these products, attackers might exploit this vulnerability to decrypt the encrypted messages and/or initiate a Man-in-the-middle (MITM) attack.

Array Networks AVX and WAN Series products as well as APV/vAPV and AG/vxAG Series products that are not using any SSL hardware card are thus not affected by this vulnerability.

Workaround

ArrayOS APV 8.6.0.x versions and ArrayOS AG 9.4.0.x versions support ECDHE cipher suites. On Array products running these versions, disabling the RSA cipher suites and using only ECDHE cipher suites can eliminate this vulnerability. Please note that this workaround may affect the access of legacy clients that do not support ECDHE cipher suites.

ArrayOS APV 8.5.0.x versions and ArrayOS AG 9.3.0.x versions do not support ECDHE cipher suites. Therefore, this workaround does not apply to Array products running these

versions. To use this workaround, you need to upgrade the system to ArrayOS APV 8.6.0.x or ArrayOS AG 9.4.0.x first.

Status

The following table lists the affected products, software versions and features. You can use this table to check whether your Array products are affected by this vulnerability.

Product	Affected Versions	Affected Features/Modules
APV/vAPV	All ArrayOS APV 8.6.0.x versions All ArrayOS APV 8.5.0.x versions	HTTPS/FTPS/TCPS virtual service
AG/vxAG	All ArrayOS AG 9.4.0.x versions All ArrayOS AG 9.3.0.x versions	Virtual site

Solution

For APV/vAPV and AG/vxAG Series products, new ArrayOS versions will be released to address this vulnerability.

➢ **Available ArrayOS APV Version**

- APV 8.6: The solution is available in the ArrayOS APV 8.6.0.104 version that has been released on December 29, 2017.
- APV 8.5: The solution will be available in a future ArrayOS APV 8.5.0.x release.

➢ **Available ArrayOS AG Version**

- AG 9.4: The solution is available in the ArrayOS AG 9.4.0.188 version that has been released on December 29, 2017.
- AG 9.3: The solution will be available in a future ArrayOS AG 9.3.0.x release.