Array Networks Security Advisory: OpenSSL CVE-2015-0204 Vulnerability (FREAK)

Advisory Date: March 23, 2015

Vulnerability Overview

The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct RSA-to-EXPORT_RSA downgrade attacks and facilitate brute-force decryption by offering a weak ephemeral RSA key in a noncompliant role. An attacker could exploit the vulnerability by returning a weak temporary RSA key using the vulnerable OpenSSL library. This vulnerability has been assigned CVE ID CVE-2015-0204 and is referred as "FREAK".

Impact

The insecure temporary key may allow the attackers to bypass secure restrictions.

Status

- ***For APV Series products, the HTTPS/TCPS/FTPS virtual services, WebUI, XML-RPC and SOAP API are not affected.***
- ***For AG Series products, the virtual sites, WebUI and XML-RPC are not affected.***
- For TMX Series and APVx200 Series products, the HTTPS/TCPS/FTPS virtual services with any EXP cipher suite enabled are affected in TM 6.5.2.x releases, and WebUI and XML-RPC are affected before the ArrayOS TM 6.5.2.36 release. ***The administrator can disable the EXP cipher suites manually.***
- For SPX Series products, the virtual sites with any EXP cipher suite enabled are affected in the SPX 8.4.6.2.x releases, while WebUI and XML-RPC are not affected. ***The administrator can disable the EXP cipher suites manually.***
- For aCelera™/WAN Series products, the SSL optimization function and WebUI are affected in the WAN 4.x releases.

Product	**Affected Versions**	**Affected Features/Modules**
TMX/APV(x200)	All ArrayOS TM 6.5.2.x	HTTPS/TCPS/FTPS virtual service
	All ArrayOS TM 6.5.2.x before ArrayOS TM 6.5.2.36	WebUI and XML-RPC
SPX	All ArrayOS SPX 8.4.6.2.x	Virtual site
WAN	All ArrayOS WAN 4.x	SSL optimization WebUI

Mitigation

- **ArrayOS TM Mitigation Measure**

For the TMX and APVx200 Series products, to avoid attacks on the HTTPS/TCPS/FTPS virtual services, execute the "**ssl settings ciphersuite**" command to disable the EXP cipher suites; to avoid attacks on WebUI and XML-RPC, upgrade the system to ArrayOS TM 6.5.2.36 or later.

- **ArrayOS SPX Mitigation Measure**

For the SPX Series products, to avoid attacks on the virtual sites, execute the "**ssl settings ciphersuite**" command to disable the EXP cipher suites.

Array Networks Solution

For TMX/SPX/WAN, new ArrayOS versions will be released to address this vulnerability.

- **Available ArrayOS TM Version**

The solution will be available in the future ArrayOS TM 6.5.2.x version.

- **Available ArrayOS SPX Version**

The solution will be available in the future ArrayOS SPX 8.4.6.2 version.

- **Available ArrayOS WAN Version**

The solution will be available in the future ArrayOS WAN 4.x version.