Array Networks Security Advisory for SSLv3 Vulnerability CVE-2014-3566

Advisory Date: October 20, 2014

Vulnerability Overview

A vulnerability in the design of Secure Socket Layer (SSL) version 3.0 has been discovered that may allow a network attacker to force a client to negotiate an SSL handshake using the SSLv3 protocol instead of Transport Layer Security (TLS) version 1.x. This is an industry-wide vulnerability affecting the SSLv3 protocol itself and is not specific to the ArrayOS.

Impact

In this man-in-the-middle (MiTM) attack, an attacker could downgrade an encrypted TLS session by forcing clients to use SSLv3 and then forcing the browser to execute malicious code. This code sends several requests to a target HTTPS website that sends cookies automatically if a previously authenticated session exists. This is a required condition for exploiting this vulnerability. The attacker could then intercept this HTTPS traffic and decrypt portions of the encrypted traffic (for example authentication cookies) by exploiting a weakness in the CBC block cypher in SSLv3. Considering the low feasibility of the attack, this vulnerability is considered **low risk**.

Status

In the APV/AG products, the **virtual services** (HTTPS, FTPS and TCPS) or **virtual sites** have SSLv3:TLSv1.0:TLSv1.2 enabled by default and therefore are affected. ***SSLv3 can be disabled for virtual services or virtual sites by the administrator manually.***

In the TMX/SPX products, the **virtual services** (HTTPS, FTPS and TCPS) or **virtual sites** have SSLv3:TLSv1.0 enabled by default and therefore are affected. ***SSLv3 can be disabled for virtual services or virtual sites by the administrator manually.***

In the WAN product, the aCelera **SSL acceleration** has SSLv3:TLSv1.0 enabled by default and therefore is affected. ***SSLv3 cannot be disabled by the administrator manually.***

In the APV/TMX/AG/SPX/WAN products, **management services** (WebUI/XMLRPC/SOAP API) have SSLv3:TLSv1:TLSv1.1 enabled by default and therefore are affected. ***SSLv3 cannot be disabled by the administrator manually.***

Product	Affected Versions	Affected Features/Modules
APV(x600)	All ArrayOS APV 8.x	HTTPS, FTPS and TCPS virtual services Management services
TMX/APV(x200)	All ArrayOS TM 6.x	HTTPS, FTPS and TCPS virtual services Management services
AG	All ArrayOS AG 9.x	Virtual site Management services
SPX	All ArrayOS SPX 8.x	Virtual site Management services
WAN	All ArrayOS WAN 4.2.x	SSL acceleration Management services

Mitigation

Disabling the SSLv3 protocol is the recommended way to avoid this attack.
For the virtual services and virtual sites in the APV/TMX/AG/SPX product, you can take the following mitigation measures to avoid this attack:

➢ **ArrayOS APV and TMX Mitigation Measures**

In the APV product, execute the command "**ssl settings protocol** <*vhost*> <*ssl_version*>" to set the SSL version as "TLSv1:TLSv12" to disable SSLv3.

In the TMX product, execute the command "**ssl settings protocol** <*vhost*> <*ssl_version*>" to set the SSL version as "TLSv1" to disable SSLv3.

➢ **ArrayOS AG and SPX Mitigation Measures**

In the AG product, execute the command "**ssl settings protocol** <*ssl_version*>" to set the SSL version as "TLSv1:TLSv12" to disable SSLv3.

In the SPX product, execute the command "**ssl settings protocol** <*ssl_version*>" to set the SSL version as "TLSv1" to disable SSLv3.

Note: In the APV/TMX/AG/SPX products, the SSL service should be stopped first before changing the SSL version. Therefore, services will be interrupted when configuration changes are made.

For the management services in the APV/TMX/AG/SPX/WAN product and the SSL acceleration in the WAN product, no mitigation measure is available. The administrator can only upgrade the system to a new version that contains the solution.

Array Networks Solution

To eliminate the risk of attacks by exploiting this vulnerability, Array Networks will implement the solution as follows:

- Disable SSLv3 for virtual services and virtual site by default in the APV/TMX/AG/SPX products.
- Disable SSLv3 for management services in the APV/TMX/AG/SPX products.
- Disable SSLv3 for SSL acceleration in the WAN products.

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

➢ **Available ArrayOS APV/TMX Versions**

The solution will be available from the following ArrayOS APV/TM versions:

- Future ArrayOS APV 8.5.1.x release
- Future ArrayOS APV 8.5.0.x release
- Future ArrayOS APV 8.4.1.x release
- Future ArrayOS APV 8.4.0.x release
- Future ArrayOS TM 6.5.2.x release

➢ **Available ArrayOS AG/SPX Versions**

The solution will be available from the following ArrayOS AG/SPX versions:

- Next ArrayOS AG 9.3.0.x release
- Next ArrayOS SPX 8.4.6.2.x release

➢ **Available ArrayOS WAN Versions**

The solution will be available from the following ArrayOS WAN version:

- Next ArrayOS WAN 4.2.x release