SECURITY ADVISORY

#CVE-2016-0777 and CVE-2016-0778 published on January 14th, 2016

Summary Description

This security advisory addresses CVE-2016-0777 and CVE-2016-0778 as they pertain to A10 ACOS software. Those vulnerabilities can affect both the server and client side. In ACOS roaming is disabled by default on the server side but not on the client side.

Details

On January 14th, Qualys, released two security advisories (CVE-2016-0777 and CVE-2016-0778) pertaining to OpenSSH. The first advisory has to do with the disclosure of memory regions, which in turn can lead to disclosure of cryptographic key material or other sensitive information, and the second has to do with disclosure of file descriptors, which has not particular application in ACOS.

Both vulnerabilities pertain to the use of the roaming feature which in ACOS is supported on the server side and is supported on the client side, thus there is inherent risk associated with the use of the ACOS ssh command outbound to a malicious or compromised server.

Mitigation Recommendations

The SSH service on ACOS is not vulnerable so there is no need for mitigation.

The client ACOS command can be exploited if the user connects to an ACOS box and from it initiates SSH connection to a SSH server that is malicious or compromised. It is advised, that until the Software Updates are installed, users do not SSH from an ACOS system to other systems and especially if those systems are not under their control and trusted to not be compromised. See the **Software Updates** section for more details.

Vulnerability Assessment

Affected Platforms: *ADC, CGN, TPS*

Affected Software Versions: *4.x, 3.x, 2.7.2-Px, 2.7.1-GR1, 2.8.2-Px*

Software Updates

Software updates resolving this vulnerability will be published at the following URL when available:

http://www.a10networks.com/support-axseries/downloads/downloads.php

The following table summarizes update versions resolving all of the above CVEs.

Vulnerable Release	Resolved Release
2.7.1-GR1	2.7.1-GR1-P1
2.7.2-Px	2.7.2-P8
2.8.2-Px	2.8.2-P5
3.x	3.2.1
4.x	4.1.0

References

1. Qualys Security advisory on CVE-2016-0777 and CVE-2016-0778: https://www.qualys.com/2016/01/14/cve-2016-0777-cve-2016-0778/openssh-cve-2016-0777-cve-2016-0778.txt