RAPID RESPONSE

ACOS Buffer Overflow Vulnerability Issued by NCCIC/US Cert Week of June 2, 2014

Summary Description

On June e, 2014, the NCCIC/US CERT issued a vulnerability summary of a classified Medium level vulnerability in ACOS.

> Buffer overflow in A10 Networks Advanced Core Operating System (ACOS) before 2.7.0-p6 and 2.7.1 before 2.7.1-P1_55 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long session id in the URI to sys_reboot.html. NOTE: some of these details are obtained from third party information.

This is a known vulnerability. There are fixes for all versions of ACOS. The recommended mitigations are to upgrade to the patched releases and limit management access to a restricted internal networks.

Vulnerability Assessment

Affected Platforms: *ADC, CGN, TPS*

Affected Software Versions: *2.6.1-GR1-X, 2.7.X, 2.6.6-GR1-x, 2.8.0, TPS 2.9.1*

ADC codes prior to version 2.7.2, 2.7.1-P1, 2.7.0-P3, and 2.6.1-GR1-p9 are vulnerable. CGN codes prior to 2.6.6-GR1-P5 and 2.8.0 are vulnerable to this exploit. TPS codes 2.9.1 are vulnerable to this exploit.

A10 Software defect id 128069 documents this vulnerability.

Mitigation Recommendations

A10 Networks recommends upgrading to the latest available patch release.

Technology	Major Release	Fixed	Latest Patch
ADC	2.7.2	2.7.2	2.7.2-P1
ADC	2.7.1	2.7.1-P1	2.7.1-P5
ADC	2.7.0	2.7.0-P3	2.7.0-P6
ADC	2.6.1-GR1-X	2.6.1-GR1-P9	2.6.1-GR1-P12
CGN	2.6.6-GR1-X	2.6.6-GR1-P5	2.6.6-GR1-P5
CGN	2.8.0	2.8.0	2.8.0-P4
TPS	3.0.0*	3.0.0	3.0.0-TPS-P1
TPS	2.9.1	2.9.1-P2-SP7	2.9.1-P2-SP7

* *Not vulnerable to this particular issue, but a later version is available.*

As a workaround, A10 customers should restrict the access to the management interface with access-control lists. By default, the A10 data interfaces have WebUI turned off. If WebUI access is enabled on the data interfaces, it is recommended to restrict the access with access-control lists.