SECURITY ADVISORY

"Shellshock Bash" #CVE-2014-6271 published on Sept. 24, 2014

UPDATED September 30 with these changes: • This is the *final advisory* that will be published on the single #CVE-2014-6271and are publishing a "rolling advisory" titled "Shellshock Bash Multiple CVEs" on our Support   Portal   [https://www.a10networks.com/support-axseries/downloads/downloads.php#CVE-2014-6271] to cover the additional CVEs that have been spawned as a results of the initial vulnerability. We are continuing to monitor and are testing all new exploit vectors of this bug as they evolve. • At this point, we have not been able to exploit any A10 systems, but will continue to test and report on new vectors and/or vulnerabilities via the separate advisory referenced above. • We have also made patches available for all our ADC and CGN products and versions of ACOS (please see the Patch Information chart below. Patches are available to A10 support customers via our Support Portal). In addition, we will be including patches for any new exploits in our regularly scheduled code releases.

UPDATED September 26 with these changes: • Version numbers added for HVA and aGalaxy • ADC version 2.4.3 removed (it is EOL) • "Protecting Other Devices Using aFleX" subtitle added for further clarification • Minor typo corrected on p. 2 (from "is" to "it")

Summary Description

On September 24th, 2014, CVE-2014-6271 (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271) was published, revealing a major issue with the way GNU Bash processes environment variables. More specifically, Bash does not properly parse functions passed in environment variables, allowing trailing code to be executed in the Bash context. This allows an attacker to execute arbitrary code by properly crafting environment variables.

In general, this bug can be triggered over the network without authentication, which makes it extremely sensitive, and is currently ranked with the highest possible CVSS v2 base score of 10, according to the National Vulnerability Database.

A10 Networks has not been able to replicate this condition *remotely* with A10 Thunder, AX, ID, or EX Series products. However, we are still researching several corner cases and we will update this advisory as we have new information.

However, *local exploitation* is possible and we will be, therefore, providing patches to address this issue (see below for information on how to download patches).

There is an ongoing discussion of additional issues stemming from the way Bash parses variable content that are currently tracked under CVE-2014-7169 (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-

2014-7169). Our team is continuously monitoring those developments and, if A10 products are deemed to be vulnerable to any of the issues addressed in CVE-2014-7169, A10 will provide patches for those as well.

Details

GNU Bash through version 4.3 is affected with this vulnerability.

Vulnerable versions of Bash are used in A10's products. Our engineers have been able to validate that in the current configuration, it is possible to execute and trigger this vulnerability locally. For most deployments, this is not an issue since access to the systems is usually authenticated and the operator is already at the highest level of privileges.

We are further investigating the issue and will provide updates as we complete our investigation.

From the point of view of remote exploitation, there are a couple of mitigating factors that suggest this vulnerability may not be triggered; however, we cannot rule this out as a possibility.

The first factor is that none of our web-based management processes use the CGI interface, nor do our other management processes spawn Bash to perform their tasks. This makes it very unlikely that a tainted variable will propagate and be provided in environments where Bash will be executed.

The second mitigating factor is that none of the management interfaces are exposed to the data plane. At this point, the only point of contact would be the management plane, which by definition, is much better guarded and access is limited.

Vulnerability Assessment

Affected Platforms: ADC, CGN, TPS, AX, ID, EX, aGalaxy, HVA

Affected Software Versions: ADC 2.6.1-GR1-X, 2.7.X, CGN 2.6.6-GR1-x, 2.8.x, TPS 2.9.1, 3.0

ADC codes prior to version 2.6.1-GR1-X and 2.7.X are vulnerable. CGN codes prior to 2.6.6-GR1-x and 2.8.x are vulnerable to this exploit. TPS codes 2.9.1 and 3.0 are vulnerable to this exploit.

A10 Software defect id 213895 documents this vulnerability.

Mitigation Recommendations & Patch Information

We will be providing updates for all versions of ACOS beginning this evening (Sept. 25, 2014), prioritizing our most broadly deployed releases first and working through to completion. Customers and partners are encouraged to visit A10's Support Portal and check for additional patches over the next few weeks as the vulnerabilities evolve with public discourse.

Technology	Major Release	Fixed
AD	2.6.1---GR1---P13	2.6.1---GR1---P13---sp2
AD	2.7.0---P6	2.7.0---P6---SP3
AD	2.7.1---P5	2.7.1---P5---SP6
AD	2.7.2---P2	2.7.2---P2---SP6
CG	2.6.6---GR1---P5	2.6.6---GR1---P5---SP1
CG	2.8.0---P4	2.8.0---P4---SP1
CG	2.8.1---P2	2.8.1---P2---SP1
CG	2.8.2	2.8.2---SP1
TPS	3.0---P2	3.0---P2---sp4
HVA	2.7.2---P2	2.7.2---P2---SP6
aGalaxy	2.5.2---P2	2.5.2---P3 (available 10.2.14)

Work-Around:

As an immediate workaround, A10 customers should restrict access to the management interface with access-control lists. By default, because A10 products provide an out-of-band management interface, remote users connected to networking — or data plane — ports would not be able to access the Web user interface. If Web user interface access is enabled on data plane interfaces, it is recommended to restrict the access with access-control lists.

Example:

Applying an access-list will prevent unknown IP addresses from accessing the A10 device and management services.

```
access-list 134 deny icmp any any
access-list 134 deny tcp any any eq 23
access-list 134 deny tcp any any eq 80
access-list 134 permit tcp 172.0.0.0 0.255.255.255 host 10.150.144.170 eq 22
access-list 134 permit tcp 172.0.0.0 0.255.255.255 host 10.150.144.170 eq 443
access-list 134 deny ip any any

AX2600(config)#interface    management
AX2600(config-if:management)#   access-list   134
```

Protecting Other Devices Using aFleX

For customers who have CGI scripts running in their application environment, A10 recommends utilizing the following aFleX script to mitigate the known attack vector. This aFleX rule can be applied to HTTP and HTTPS Virtual Ports. A10 does recommend evaluation of the script for possible performance impacts if the specific platform currently has high CPU loads. The aFleX script has not been benchmarked for performance. This script may be updated periodically if new information is gathered about this threat.

aFleX rules for protecting origin servers with vulnerable services

```
when HTTP_REQUEST {

if {[HTTP::request] contains "() \{"} {
log "Detected CVE-2014-6271 attack in a request from [IP::client_addr]
request was [HTTP::request]"
TCP::close
drop
}
if {[HTTP::query] contains "() \{"} {
log "Detected CVE-2014-6271 attack in a request from [IP::client_addr]
query was [HTTP::query]"
TCP::close
drop
}
if {[HTTP::header count] > 0} {
foreach req_header [HTTP::header names] { if {[HTTP::header values
$req_header] contains "() \{" } { log "Detected CVE-2014-6271 attack in a
request from [IP::client_addr] in
header: $req_header"
TCP::close
drop
}
}
}
if {[ HTTP::cookie count] > 0} {
foreach r_cookie [HTTP::cookie names] {
if {[HTTP::cookie value $r_cookie] contains "() \{" } { log "Detected
CVE-2014-6271 attack in a request from [IP::client_addr] in
Cookie: $r_cookie"
TCP::close
drop
}
}
}
}
```