Interactive Northwest, Inc.
7672 SW Mohawk Street
Tualatin, OR 97062

INI Applications and the "Shellshock" bug in BASH

This document is intended to assist in the description, diagnosis, and remediation of the BASH bug known as “Shellshock” as it relates to systems with INI applications installed.

Description of Shellshock

On September 24th, 2014 a bug that affected the BASH package included in Red Hat Linux operating systems was made public. This bug could allow for arbitrary code execution. “Shellshock” has been assigned a Common Vulnerabilities number of CVE-2014-6271 and CVE-2014-7169
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7169

The following is a description of the bug, quoted from CVE-2014-6271:

“GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "ShellShock." NOTE: the original fix for this issue was incorrect; CVE-2014-7169 has been assigned to cover the vulnerability that is still present after the incorrect fix.”

Vendor Statements

Red Hat

“This issue affects all products which use the Bash shell and parse values of environment variables. This issue is especially dangerous as there are many possible ways Bash can be called by an application. Quite often if an application executes another binary, Bash is invoked to accomplish this. Because of the pervasive use of the Bash shell, this issue is quite serious and should be treated as such.
All versions prior to those listed as updates for this issue are vulnerable to some degree.
See the appropriate remediation article for specifics.”

https://access.redhat.com/security/cve/CVE-2014-6271
https://access.redhat.com/security/cve/CVE-2014-7169
https://access.redhat.com/articles/1200223
https://securityblog.redhat.com/2014/09/24/bash-specially-crafted-environment-variables-code-injection-attack/

Avaya

Avaya has released a Security Advisory in response to the “Shellshock” vulnerability. Careful review of the advisory and any related documentation is necessary for each environment where and Avaya product exists.

https://downloads.avaya.com/css/P8/documents/100183009

Avaya is releasing patches for the various products that are affected by this vulnerability, refer to the “Actions” column in the linked document above for more specific information.

Avaya’s recommended action for system products is quoted from the above link:

“Avaya strongly recommends following networking and security best practices by implementing firewalls, ACLs, physical security or other appropriate access restrictions. Though Avaya believes such restrictions should always be in place, risk to Avaya products and the surrounding network from this potential vulnerability may be mitigated by ensuring these practices are implemented until such time as an Avaya provided product update or the recommended Avaya action is applied. Further restrictions as deemed necessary based on the customer's security policies may be required during this interim period, but the System Product operating system or application should not be modified unless the change is approved by Avaya. Making changes that are not approved may void the Avaya product service contract.”

INI Applications

The standard installation platform used by INI is affected by this vulnerability. Due to the impact this vulnerability could have on the security of an environment, INI recommends following Red Hat’s procedures to update the affected package.

Diagnosis of Shellshock

To determine if a Red Hat Linux system is affected by this vulnerability follow the steps below.

1. Gain shell access to the server and log in.
2. Run the following command to determine which version of BASH is installed:
    a. rpm -q bash
3. Compare the results to the version information provided by Red Hat detailing affected packages. (CVE-2014-6271,CVE-2014-7169,RHSA-2014:1311, RHSA-2014:1306, RHSA-2014:1312)

To verify that the vulnerability exists, run the following command in a bash shell:

```
env x='() { :;}; echo vulnerable'  bash -c "echo this is a test"
```

If the following appears, the system is affected:

```
vulernable
this is a test
```

Please continue to reference Red Hat documentation of this issue for vulnerabilities, diagnosis, and remediation instructions.

Remediation of Shellshock

For non-Avaya Red Hat systems, follow the remediation instructions provided by Red Hat. The current remediation may not be comprehensive, as noted in CVE-2014-6271.

For Avaya systems affected by this vulnerability, read the following documents and follow the Reccommended Actions given by avaya:

Avaya Security Vulnerability Classification Policy
https://support.avaya.com/css/P8/documents/100066674

Avaya Security Vulnerability Response Policy
https://support.avaya.com/css/P8/documents/100045520

Avaya Security Advisory (ASA-2014-369)
https://downloads.avaya.com/css/P8/documents/100183009

This document will be updated as needed.