ACS evaluation for CVE-2014-6271 and CVE-2014-7169

CSCur00511

Description

The Cisco Secure Access Control Server (ACS) includes a version of bash that is affected by the vulnerabilities  
identified by the Common Vulnerability and Exposures (CVE) IDs:  
  
CVE-2014-6271  
CVE-2014-7169  
  
This bug has been opened to address the potential impact on this product.  
Analysis from development team:  
All shipping versions of ACS are vulnerable CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187 , CVE-2014-6277 and CVE-2014-6278 (AKA ShellShock bug). ACS patch will be made available for all supported versions of ACS in a timely manner. That said, the exposure of this bug in ACS is very limited. The shellshock vulnerability allows an SSH AUTHENTICATED user run a generic Linux command. The key word being 'AUTHENTICATED'. Hence if an attacker does not have the username and password of an ACS CLI user, they will not be able to exploit this vulnerability on ACS.   
  
If the user DOES have credentials, and would like to exploit the shellshock, that CLI user would be able to run generic Linux commands on the ACS Server that would normally not be able to run (Because the ACS CLI does not expose generic Linux commands). However those Linux commands will run as the logged in CLI user account, not as the Linux root user. Hence, this limits exposure of the vulnerability in ACS. An example of an exploit using shellshock in ACS would be to view Linux system files they would normally not be able to view.   
  
The workaround to remove the vulnerability would be to disable the SSH daemon via the following CLI, then reload the ACS server to ensure all SSH sessions have been terminated. The following CLI demonstrates how to to disable SSH service and reload the node:  
  
---snip  
acs1/admin# configure terminal  
acs1/admin(config)# no service sshd enable   
acs1/admin(config)# end  
acs1/admin# reload  
Save the current ADE-OS running configuration? (yes/no) [yes] ? yes  
Continue with reboot? [y/n] y  
---snip  
  
  
Disable SSH as follows (until the ACS patch with the fix for [CSCur00511](https://bst.cloudapps.cisco.com/bugsearch/bug/CSCur00511/CSCur00511) is installed):  
  
---snip  
acs1/admin# configure terminal  
acs1/admin(config)# no service sshd enable   
acs1/admin(config)# end  
acs1/admin# reload  
Save the current ADE-OS running configuration? (yes/no) [yes] ? yes  
Continue with reboot? [y/n] y  
---snip  
  
  
The other work around can be restrict IP addresses to access CLI of ACS only for known admin laptops by making configuration change on end switch /firewall device where ACS is connected .  
  
For example:   
tcp permit   
tcp deny any   
permit rest   
  
  
 **The Cisco Secure Access Control Server (ACS) includes a version of bash that is affected by the vulnerabilities  
identified by the Common Vulnerability and Exposures (CVE) IDs:  
  
CVE-2014-6271  
CVE-2014-7169  
  
This bug has been opened to address the potential impact on this product.  
Analysis from development team:  
All shipping versions of ACS are vulnerable CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187 , CVE-2014-6277 and CVE-2014-6278 (AKA ShellShock bug). ACS patch will be made available for all supported versions of ACS in a timely manner. That said, the exposure of this bug in ACS is very limited. The shellshock vulnerability allows an SSH AUTHENTICATED user run a generic Linux command. The key word being 'AUTHENTICATED'. Hence if an attacker does not have the username and password of an ACS CLI user, they will not be able to exploit this vulnerability on ACS.   
  
If the user DOES have credentials, and would like to exploit the shellshock, that CLI user would be able to run generic Linux commands on the ACS Server that would normally not be able to run (Because the ACS CLI does not expose generic Linux commands). However those Linux commands will run as the logged in CLI user account, not as the Linux root user. Hence, this limits exposure of the vulnerability in ACS. An example of an exploit using shellshock in ACS would be to view Linux system files they would normally not be able to view.   
  
The workaround to remove the vulnerability would be to disable the SSH daemon via the following CLI, then reload the ACS server to ensure all SSH sessions have been terminated. The following CLI demonstrates how to to disable SSH service and reload the node:  
  
---snip  
acs1/admin# configure terminal  
acs1/admin(config)# no service sshd enable   
acs1/admin(config)# end  
acs1/admin# reload  
Save the current ADE-OS running configuration? (yes/no) [yes] ? yes  
Continue with reboot? [y/n] y  
---snip**  
Disable SSH as follows (until the ACS patch with the fix for [CSCur00511](https://bst.cloudapps.cisco.com/bugsearch/bug/CSCur00511/CSCur00511) is installed):  
  
---snip  
acs1/admin# configure terminal  
acs1/admin(config)# no service sshd enable   
acs1/admin(config)# end  
acs1/admin# reload  
Save the current ADE-OS running configuration? (yes/no) [yes] ? yes  
Continue with reboot? [y/n] y  
---snip  
  
  
The other work around can be restrict IP addresses to access CLI of ACS only for known admin laptops by making configuration change on end switch /firewall device where ACS is connected .  
  
For example:   
tcp permit   
tcp deny any   
permit rest  
  
**Symptom:**  
The Cisco Secure Access Control Server (ACS) includes a version of bash that is affected by the vulnerabilities  
identified by the Common Vulnerability and Exposures (CVE) IDs:  
  
CVE-2014-6271  
CVE-2014-7169  
  
This bug has been opened to address the potential impact on this product.  
Analysis from development team:  
All shipping versions of ACS are vulnerable CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187 , CVE-2014-6277 and CVE-2014-6278 (AKA ShellShock bug). ACS patch will be made available for all supported versions of ACS in a timely manner. That said, the exposure of this bug in ACS is very limited. The shellshock vulnerability allows an SSH AUTHENTICATED user run a generic Linux command. The key word being 'AUTHENTICATED'. Hence if an attacker does not have the username and password of an ACS CLI user, they will not be able to exploit this vulnerability on ACS.   
  
If the user DOES have credentials, and would like to exploit the shellshock, that CLI user would be able to run generic Linux commands on the ACS Server that would normally not be able to run (Because the ACS CLI does not expose generic Linux commands). However those Linux commands will run as the logged in CLI user account, not as the Linux root user. Hence, this limits exposure of the vulnerability in ACS. An example of an exploit using shellshock in ACS would be to view Linux system files they would normally not be able to view.   
  
The workaround to remove the vulnerability would be to disable the SSH daemon via the following CLI, then reload the ACS server to ensure all SSH sessions have been terminated. The following CLI demonstrates how to to disable SSH service and reload the node:  
  
---snip  
acs1/admin# configure terminal  
acs1/admin(config)# no service sshd enable   
acs1/admin(config)# end  
acs1/admin# reload  
Save the current ADE-OS running configuration? (yes/no) [yes] ? yes  
Continue with reboot? [y/n] y  
---snip  
  
**Conditions:**  
  
ACS server is exposed to this vulnerability only if they have ssh service enabled. If SSH is enabled, a remote user with ACS CLI credentials will be able to exploit the vulnerability and run generic Linux commands.  
  
 **Workaround:**  
Disable SSH as follows (until the ACS patch with the fix for [CSCur00511](https://bst.cloudapps.cisco.com/bugsearch/bug/CSCur00511/CSCur00511) is installed):  
  
---snip  
acs1/admin# configure terminal  
acs1/admin(config)# no service sshd enable   
acs1/admin(config)# end  
acs1/admin# reload  
Save the current ADE-OS running configuration? (yes/no) [yes] ? yes  
Continue with reboot? [y/n] y  
---snip  
  
  
The other work around can be restrict IP addresses to access CLI of ACS only for known admin laptops by making configuration change on end switch /firewall device where ACS is connected .  
  
For example:   
tcp permit   
tcp deny any   
permit rest  
  
**Further Problem Description:**  
**Fixed Code:**  
Patch for DDTS [CSCur00511](https://bst.cloudapps.cisco.com/bugsearch/bug/CSCur00511/CSCur00511) is ready and available on CCO.  
The patch is included in all cumulative patches from version 5.4.0.46.7/5.5.0.46.6/5.6.0.22.1 and later. We recommend that you download the latest cumulative patches.  
  
Download from: CCO / Support / Download Software <http://www.cisco.com/cisco/pub/software/portal/select.html?i=!y>  
Select: Security / Identity Management / Cisco Secure Access Control System / Cisco Secure Access Control System 5.4 / 5.4.0.46.0  
  
Patch filename: 5-4-0-46-(latest).tar.gpg  
Readme and installaion instructions: Acs-5-4-0-46-(latest)-Readme.txt  
  
Download from: CCO / Support / Download Software <http://www.cisco.com/cisco/pub/software/portal/select.html?i=!y>  
Select: Security / Identity Management / Cisco Secure Access Control System / Cisco Secure Access Control System 5.5 / 5.5.0.46  
  
Patch filename: 5-5-0-46-(latest).tar.gpg  
Readme and installaion instructions: Acs-5-5-0-46-(latest)-Readme.txt  
  
Download from: CCO / Support / Download Software <http://www.cisco.com/cisco/pub/software/portal/select.html?i=!y>  
Select: Security / Identity Management / Cisco Secure Access Control System / Cisco Secure Access Control System 5.6 / 5.6.0.22  
  
Patch filename: 5-6-0-22-(latest).tar.gpg  
Readme and installaion instructions: Acs-5-6-0-22-(latest)-Readme.txt  
  
Download from: CCO / Support / Download Software <http://www.cisco.com/cisco/pub/software/portal/select.html?i=!y>  
Select: Security / Identity Management / Cisco Secure Access Control System / Cisco Secure Access Control System 5.3 / 5.3.0.40  
  
Patch filename: 5-3-0-40-(latest).tar.gpg  
Readme and installaion instructions: Acs-53(latest)-Readme.txt  
  
  
  
**PSIRT Evaluation:**  
The Cisco PSIRT has assigned this bug the following CVSS version 2  
score. The Base and Temporal CVSS scores as of the time of evaluation  
are 7.5/7.5:  
  
<http://tools.cisco.com/security/center/cvssCalculator.x?vector=AV:N/AC:L/Au:N/C:P/I:P/A:P/E:H/RL:U/RC:C&version=2.0>  
  
The Cisco PSIRT has assigned this score based on information obtained  
from multiple sources. This includes the CVSS score assigned by the  
third-party vendor when available. The CVSS score assigned may not  
reflect the actual impact on the Cisco Product.  
  
Additional information on Cisco's security vulnerability policy can be  
found at the following URL:  
  
<http://www.cisco.com/web/about/security/psirt/security_vulnerability_policy.html>