Radware Emergency Response Team

Threat Alert: Shellshock

CVE-2014-6271, CVE-2014-7169

Version 1.0.0 Rev. 1
September 26, 2014

Table of Contents

Background

Two new vulnerabilities were recently found in Bash (CVE-2014-6271, CVE-2014-7169). These vulnerabilities potentially affect certain services and applications and allow remote unauthenticated attackers to exploit this issue and use this flaw to override or bypass environment restrictions.

This issue affects all products that use Bash and parse values of environment variables. The vulnerable Bash versions are:

1.14.0, 1.14.1, 1.14.2, 1.14.3, 1.14.4, 1.14.5, 1.14.6, 1.14.7, 2.0, 2.01, 2.01.1, 2.02, 2.02.1, 2.03, 2.04, 2.05, 2.05:b, 3.0, 3.0.16, 3.1, 3.2, 3.2.48, 4.0, 4.0:rc1, 4.1, 4.2, 4.3

Risk

The vulnerabilities potentially affect certain services and applications and allow remote unauthenticated attackers to inject certain characters into other environments, allowing them to exploit this issue and use this flaw to override or bypass environment restrictions to execute shell commands. Under certain conditions, attackers can also provide specially-crafted environment variables containing arbitrary commands that will be executed on vulnerable systems.

This issue affects products using vulnerable version as detailed in the background paragraph.

Mitigation Options

IPS Signatures

Radware Emergency Response Team (ERT) has produced two IPS signatures for the above vulnerabilities.

1. RWID: 16542
2. RWID: 16544
3. RWID: 16546
4. RWID: 16548
5. RWID: 16550
6. RWID: 16552
7. RWID: 16554
8. RWID: 16556
9. RWID: 16558
10. RWID: 16560
11. RWID: 16562
12. RWID: 16564
13. RWID: 16566
14. RWID: 16568
15. RWID: 16570
16. RWID: 16572
17. RWID: 16574
18. RWID: 16576
19. RWID: 16578

Radware ERT Recommendations

- Copy and paste both signature commands into DefensePro CLI and assign them to a protection policy. The signature will be implemented in 'Report Only' mode

- Carefully inspect false positive rates of the signatures and gain confidence such patterns do not appear normally in your environment before changing it to 'Block and Report' mode

- Radware's recommendation is to patch the vulnerable systems according to instructions provided by the vendor

Radware ERT and SOC will continue monitoring for new exploits and will release additional protections as needed.

Vendor Information

- https://securityblog.redhat.com/2014/09/24/bash-specially-crafted-environment-variablescode-injection-attack/

Additional Information

References:

- https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271

- https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7169

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION IN THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. RADWARE RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME. RADWARE EXPECTS TO UPDATE THIS DOCUMENT AS NEW INFORMATION BECOMES AVAILABLE.

Contact Information

Radware, Inc. - North America Headquarters
Lobby 1 (Visitors) and Lobby 2 (Deliveries)
575 Corporate Drive
Mahwah, NJ 07430
Tel: +1 (201) 512-9771
Toll Free: +1 (888) 234-5763
Fax: +1 (201) 512-9774
Email: info@radware.com

International Headquarters
Radware Ltd.
22 Raoul Wallenberg Street
Tel Aviv 69710, Israel
Tel: 972-3-766 8666
Fax: 972-3-766-8655
Email: info_il@radware.com

For Radware complete offices and locations please visit: http://www.radware.com/Company/Locations.aspx