RandomStorm urges customers to scan for “Shell Shock” security vulnerability

- **IT system administrators should scan all connected devices and servers running Bash Shell**-

Leeds, 26th September 2014, security and compliance company, RandomStorm, has urged IT system administrators to scan their Linux, Mac OS and UNIX OS servers and connected devices for a newly identified vulnerability that affects the Bash Shell, which is normally accessed through the command line prompt.

Open source software company, Red Hat, yesterday alerted the information security community that it had identified a security bug that allows malicious code to be executed on any device that runs on the UNIX operating system and has lines of code added inside the Bash Shell. The vulnerability has been present in the UNIX operating system for more than twenty years. Dubbed “Shell Shock”, the bug has been given a severity rating of 10 because it allows an attacker to totally compromise the affected server or device and requires a very low level of skill to launch an attack.

Writing on the Red Hat Bugzilla forum, Red Hat warns, “A flaw was found in the way Bash evaluated certain specially crafted environment variables. An attacker could use this flaw to override or bypass environment restrictions to execute shell commands. Certain services and applications allow remote unauthenticated attackers to provide environment variables, allowing them to exploit this issue.”

Red Hat engineer, Thorsten Glaser, wrote: “The import of functions from the environment is a GNU bash-only feature. Neither zsh nor mksh support this. The format GNU bash uses is that, if an imported variable begins with “() {”, it’s taken as function. For every other shell, these are just normal strings.”

The patching cycle for the Randomstorm vulnerability assessment service, xStorm, is controlled and managed by RandomStorm. As soon as Shell Shock plugins are made available, xStorm will be automatically updated.

Some, incomplete, patches have been released by Ubuntu and other Linux distributors to reduce the vulnerability. RandomStorm has advised that IT managers can test their systems and connected devices for the Shell Shock bug by running either of the checks below:

env X="() { :;} ; echo vulnerable" /bin/sh -c "echo completed"
env X="() { :;} ; echo vulnerable" `which bash` -c "echo completed"
If the device returns the response 'vulnerable' then the Bash vulnerability has been detected and a patch needs to be applied.

The following link provides details on which Bash versions are vulnerable to CVE-2014-6271: http://www.cvedetails.com/cve/CVE-2014-6271/

Commenting on the “Shell Shock” discovery, Andrew Mason, Technical Director at RandomStorm said, “We are advising all of our customers to run a scan for CVE-2014-6271 to check whether their Unix, and Linux servers and networked devices, such as cameras

and alarms contain the Bash vulnerability. We will update our xStorm service with the available patch and we have emailed our customers to provide further guidance on updating their appliances."

Detailed information about this vulnerability is available from: Red Hat Bugzilla:https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2014-6271 and www.CVEDetails.com: http://www.cvedetails.com/cve/CVE-2014-6271/

RandomStorm provides vulnerability scanning and intrusion detection products and penetration testing services to help companies to improve and continually maintain their security posture. The company is a CREST and CESG CHECK security consultancy and certified as a Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV) by the Payment Card Industry Security Standards Council.

-ends-

References:

Red Hat, Bugzilla, bug tracking forum, 14th September 2014, "https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2014-6271
CVE Details, vulnerable versions of Bash Shell, http://www.cvedetails.com/cve/CVE-2014-6271/
CNN, "Bigger than Heartbleed," Bash Bug could leave IT systems shell shocked," 24th September 2014,http://www.cnet.com/news/bigger-than-heartbleed-bash-bug-could-leave-it-systems-shellshocked/
International Business Times, "Bash Bug security threat 'bigger than Heartbleed,'" 25th September 2014:http://www.ibtimes.co.uk/bash-bug-security-threat-bigger-heartbleed-1467109
BBC, "Shell shock, 'deadly serious' new vulnerability found," 25th September 2014:http://www.bbc.co.uk/news/technology-29361794
The Register, "Hackers thrash Shell Shock bug as world races to patch hole," 25th September 2014:
http://www.theregister.co.uk/2014/09/25/shellshock_bash_worm_type_fears/

About RandomStorm

RandomStorm is a UK-based network security, vulnerability management and compliance company, focused on providing enterprise-level, proactive security management tools and services. RandomStorm's experienced and certified security experts are able to offer customers a wide range of integrated world-class security vulnerability assessment and professional security services. Covering initial consultancy and gap analysis through to network and application testing, as well as managing client's business compliance accreditation process, RandomStorm aims to work with organisations to ensure that their security investment is fully optimised on a 24/7/365 basis.

RandomStorm's core products are supported by a range of complementary monitoring, alerting and remediation tools and services developed under the RandomStorm Open Source Initiative RandomStorm is a **CESG CHECK** security consultancy as well as a Qualified Security Assessor (QSA) and an Approved Scanning Vendor (ASV) for the Payment Card Industry Data Security Standard (PCI DSS). Please visit http://www.randomstorm.com for further information.