

May 26, 2015

Bash Environment Variable Injection Vulnerability Statement for Brocade

Revision 2.0

Vulnerabilities:

CVE-2014-6271: Bash Environmental Variable Command Injection Vulnerability

CVE-2014-7169: Additional Fix for Bash Command Injection Vulnerability

CVE-2014-6277: This vulnerability exists because of an incomplete fix for CVE-2014-6271 and CVE-2014-7169

CVE-2014-7186 : The redirection implementation in parse.y in GNU Bash through 4.3 bash43-026 allows remote attackers to cause a denial of service (out-of-bounds array access and application crash) or possibly have unspecified other impact via crafted use of here documents, aka the "redir_stack" issue

CVE-2014-7187: The redirection implementation in parse.y in GNU Bash through 4.3 bash43-026 allows remote attackers to cause a denial of service (out-of-bounds array access and application crash) or possibly have unspecified other impact via crafted use of here documents, aka the "redir_stack" issue

CVE-2014-6278 : NVD information is pending

Vulnerability Statement: ([Statement from Red Hat](#)) 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.

Brocade Products: For information regarding impact and resolution for Brocade products please refer to **TSB 2014-199-A** which can be obtained from your account team or on [MyBrocade.com](#). This document will be updated as more information is available to please check for updates.

Brocade Monitoring, Analytics, and Remote Troubleshooting Environment

- The Network components, i.e., firewall, switching, routing and mgmt. platform are not vulnerable.
- The Managed File Transfer was affected and system has been patched. Access Control (SSL-VPN) authentication is impacted; RSA is working on the UNIX patch.
- The UNIX/LINUX operating systems have been patched.

Brocade IT

- IT has completed patching the Internet publicly-facing UNIX/LINUX/Solaris systems (in our DMZs) as well as all internal systems.

Red Hat has posted a [security blog FAQ](#) to answer many questions about the vulnerability. Additional information regarding patches or workarounds to address this vulnerability will be forthcoming. This notice will be updated with new information when available.

Disclaimer

THIS DOCUMENT IS PROVIDED ON AN AS-IS BASIS SOLELY FOR INFORMATIONAL PURPOSES AND DOES NOT IMPLY ANY KIND OF GUARANTY OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. YOUR USE OF THE INFORMATION CONTAINED HEREIN IS AT YOUR OWN RISK. ALL INFORMATION PROVIDED HEREIN IS BASED ON BROCADE'S CURRENT KNOWLEDGE AND UNDERSTANDING OF THE VULNERABILITY AND IMPACT TO BROCADE HARDWARE AND SOFTWARE PRODUCTS.
BROCADE

1.0	First release
2.0	Updated IT status

RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.