**Title** Security Bulletin: Vulnerabilities in Bash affect IBM SDN VE (CVE-2014-6271, CVE-2014-7169, CVE-2014-7186, CVE-2014-7187, CVE-2014-6277, CVE-2014-6278)

**Summary** Six Bash vulnerabilities were disclosed in September 2014. This bulletin addresses the vulnerabilities that have been referred to as “Bash Bug” or “Shellshock” and two memory corruption vulnerabilities. Bash is used by IBM SDN VE.

## Vulnerability Details

**CVE-ID**: CVE-2014-6271

**DESCRIPTION**: GNU Bash could allow a remote attacker to execute arbitrary commands on the system, caused by an error when evaluating specially-crafted environment variables passed to it by the bash functionality. An attacker could exploit this vulnerability to write to files and execute arbitrary commands on the system.

CVSS Base Score: 10.0
CVSS Temporal Score: See **http://xforce.iss.net/xforce/xfdb/96153** for the current score
CVSS Environmental Score*: Undefined
CVSS Vector: (AV:N/AC:L/Au:N/C:C/I:C/A:C)

**CVE-ID**: CVE-2014-7169

**DESCRIPTION**: GNU Bash could allow a remote attacker to execute arbitrary commands on the system, caused by an incomplete fix related to malformed function definitions in the values of environment variables. An attacker could exploit this vulnerability using attack vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server to write to files and execute arbitrary commands on the system.

CVSS Base Score: 10.0
CVSS Temporal Score: See **http://xforce.iss.net/xforce/xfdb/96209** for the current score
CVSS Environmental Score*: Undefined
CVSS Vector: (AV:N/AC:L/Au:N/C:C/I:C/A:C)

**CVE-ID**: CVE-2014-7186

**DESCRIPTION**: GNU Bash could allow a local attacker to execute arbitrary code on the system, caused by an out-of-bounds memory access while handling redir_stack. An attacker could exploit this vulnerability to execute arbitrary code on the system or cause a denial of service.

CVSS Base Score: 4.6
CVSS Temporal Score: See http://xforce.iss.net/xforce/xfdb/96237 for the current score

CVSS Environmental Score*: Undefined
CVSS Vector: (AV:L/AC:L/Au:N/C:P/I:P/A:P)

**CVE-ID**: CVE-2014-7187

**DESCRIPTION**: GNU Bash could allow a local attacker to execute arbitrary code on the system, caused by an off-by-one-error when handling deeply nested flow control constructs. An attacker could exploit this vulnerability to execute arbitrary code on the system or cause a denial of service.

CVSS Base Score: 4.6
CVSS Temporal Score: See http://xforce.iss.net/xforce/xfdb/96238 for the current score
CVSS Environmental Score*: Undefined
CVSS Vector: (AV:L/AC:L/Au:N/C:P/I:P/A:P)

CVE-2014-6277

**DESCRIPTION**: GNU Bash could allow a remote attacker to execute arbitrary code on the system, caused by an incomplete fix related to the failure to properly parse function definitions in the values of environment variables. An attacker could exploit this vulnerability using attack vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server to execute arbitrary code on the system or cause a denial of service.

CVSS Base Score: 10.0
CVSS Temporal Score: See http://xforce.iss.net/xforce/xfdb/96686 for the current score
CVSS Environmental Score*: Undefined
CVSS Vector: (AV:N/AC:L/Au:N/C:C/I:C/A:C)

CVE-2014-6278

**DESCRIPTION**: GNU Bash could allow a remote attacker to execute arbitrary code on the system, caused by an incomplete fix related to the parsing of user scripts. An attacker could exploit this vulnerability to execute arbitrary code on the system or cause a denial of service.

CVSS Base Score: 10.0
CVSS Temporal Score: See http://xforce.iss.net/xforce/xfdb/96687 for the current score
CVSS Environmental Score*: Undefined
CVSS Vector: (AV:N/AC:L/Au:N/C:C/I:C/A:C)

## Affected Products and Versions

IBM SDN VE, Unified Controller, VMware Edition: 1.2.0 and earlier
IBM SDN VE, Unified Controller, KVM Edition: 1.2.0 and earlier
IBM SDN VE, Unified Controller, OpenFlow Edition: 1.2.0 and earlier
IBM SDN VE, Dove Management Console, VMware Edition: 1.0.0
IBM SDN VE, Service Appliance, VMware Edition: 1.2.0 and earlier
IBM SDN VE, Service Appliance, KVM Edition: 1.2.0 and earlier

## Remediation/Fixes

IBM recommends updating affected IBM SDN VE, Unified Controllers and IBM SDN VE, Service Appliances to the latest versions of IBM SDN VE for which IBM is providing a fix, which are identified below:

IBM SDN VE, Unified Controller, VMware Edition: version 1.2.1 or later
IBM SDN VE, Unified Controller, KVM Edition: version 1.2.1 or later
IBM SDN VE, Unified Controller, OpenFlow Edition: version 1.2.1 or later
IBM SDN VE, Service Appliance, VMware Edition: version 1.2.1 or later
IBM SDN VE, Service Appliance, KVM Edition: version 1.2.1 or later

**These versions are available via Passport Advantage.**

## Workarounds and Mitigations

None known

## Reference

- *Complete CVSS Guide*
- *On-line Calculator V2*

## Related Information

IBM Secure Engineering Web Portal
IBM Product Security Incident Response Blog
Subscribe to Security Bulletins

## Acknowledgement

**None**

## Change History

09 October 2014: Original Version Published

*The CVSS Environment Score is customer environment specific and will ultimately impact the Overall CVSS Score. Customers can evaluate the impact of this vulnerability in their environments by accessing the links in the Reference section of this Security Bulletin.

## Disclaimer

According to the Forum of Incident Response and Security Teams (FIRST), the Common Vulnerability Scoring System (CVSS) is an "industry open standard designed to convey vulnerability severity and help to determine urgency and priority of response." IBM PROVIDES THE CVSS SCORES "AS IS" WITHOUT WARRANTY OF ANY KIND, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY.