Title Security Bulletin: GNU C library (glibc) vulnerability affects IBM SDN-VE Unified Controller and IBM SDN-VE Service Appliance (CVE-2015-0235)

Summary GNU C library (glibc) vulnerability that has been referred to as GHOST affects IBM SDN-VE

Unified Controller and IBM SDN VE- Service Appliance .

Vulnerability Details

CVEID: CVE-2015-0235
DESCRIPTION: The gethostbyname functions of the GNU C Library (glibc) are vulnerable to a buffer overflow. By sending a specially crafted, but valid hostname argument, a remote attacker could overflow a buffer and execute arbitrary code on the system with the privileges of the targeted process or cause the process to crash. The impact of an attack depends on the implementation details of the targeted application or operating system. This issue is being referred to as the "Ghost" vulnerability.
CVSS Base Score: 7.6
CVSS Temporal Score: See http://xforce.iss.net/xforce/xfdb/100386for the current score
CVSS Environmental Score*: Undefined
CVSS Vector: (AV:N/AC:H/Au:N/C:C/I:C/A:C)

Affected Products and Versions

IBM SDN VE, Unified Controller, KVM Edition: 1.2.2 and earlier
IBM SDN VE, Unified Controller, VMware Edition: 1.2.2 and earlier
IBM SDN VE, Unified Controller, OpenFlow Edition: 1.2.2 and earlier
IBM SDN VE, Service Appliance, KVM Edition: 1.2.2 and earlier
IBM SDN VE, Service Appliance, VMware Edition: 1.2.2 and earlier
IBM SDN VE, DOVE Management Console, VMware Edition: 1.0.0

Remediation/Fixes

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

IBM SDN VE, Unified Controller, KVM Edition: 1.2.3
IBM SDN VE, Unified Controller, VMware Edition: 1.2.3
IBM SDN VE, Unified Controller, OpenFlow edition: 1.2.3
IBM SDN VE, Service Appliance, KVM Edition: 1.2.3
IBM SDN VE, Service Appliance, VMware Edition: 1.2.3

Once updates have been applied, any process using glibc will need to be restarted. Given that nearly all system processes use glibc, rebooting after upgrading is suggested.

IBM recommends that you review your entire environment to identify vulnerable releases of glibc including your Operating Systems and take appropriate mitigation and remediation actions. Please

contact your Operating System provider for more information.

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

Acknowledgement

None

Change History

Wednesday February 11th 2015 - 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