National Computer Board

Computer Emergency Response Team of Mauritius (CERT-MU)

Targeted Security Alert

TA-2015-08

HP Virtual Connect 8Gb 24-Port FC Module running OpenSSL and Bash, Remote Denial of Service, Code Execution, Disclosure of Information

Original Issue Date: 13 March 2015

Severity Rating: High

Potential Security Impact: Remote execution of code, Disclosure of Information

Software Affected:

- HP Virtual Connect 8Gb 24-Port FC Module prior to version 3.00 (VC 4.40)

Overview:

Critical security vulnerabilities have been identified with HP Virtual Connect 8Gb 24-Port FC Module running OpenSSL and Bash.

Description:

Multiple critical vulnerabilities have been reported in HP Virtual Connect 8Gb 24-Port FC Module running OpenSSL and Bash. The vulnerabilities identified are as follows:

- OpenSSL vulnerability known as "Heartbleed" exists and can be exploited by remote attackers to cause a denial of service condition or disclosure of information.

- The SSLv3 vulnerability known as "Padding Oracle on Downgraded Legacy Encryption" (POODLE) exists and can be exploited by remote attackers to disclose information.

- The Bash Shell vulnerability known as "Shellshock" occurs and could be exploited by remote attackers to cause a Denial of Service (DoS) or execute arbitrary code.

Solution

HP has provided an update to resolve the above vulnerability. Users are advised to apply the following update:

- HP Virtual Connect 8Gb 24-Port FC Module version 3.00 (VC 4.40)

More information about the update is available on:

https://h20564.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c04595951

Vendor Information

Hewlett Packard

www.hp.com

CVE Information

CVE-2009-3555

CVE-2014-0160

CVE-2014-0195

CVE-2014-3505

CVE-2014-3506

CVE-2014-3507

CVE-2014-3508

CVE-2014-3509

CVE-2014-3510

CVE-2014-3511

CVE-2014-3512

CVE-2014-3566

CVE-2014-5139

References

HP Support Centre

https://h20564.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c04595951

Security Bulletin Archive

https://h20564.www2.hp.com/portal/site/hpsc/public/kb/secBullArchive

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378

Fax No: (+230) 208 0119

Gen. Info. : contact@cert.ncb.mu

Incident: incident@cert.ncb.mu

Website: www.cert-mu.org.mu