National Computer Board

Computer Emergency Response Team of Mauritius (CERT-MU)

Advisory

AD-2015-05

HP 3PAR Service Processor (SP) running OpenSSL and Bash, Remote Code Execution, Unauthorized Access, Disclosure of Information

Original Issue Date: 02 April 2015

Severity Rating: High

Potential Security Impact: Remote code execution, unauthorized access, disclosure of information

Software Affected:

- HP 3PAR Service Processor (SP) versions prior to SP-4.1.0.GA-97.P011, SP-4.2.0.GA-29.P003, and SP-4.3.0.GA-17.P001

Overview:

Multiple vulnerabilities have been identified in HP 3PAR Service Processor (SP) running OpenSSL and Bash and they could be exploited by remote attackers to cause execution of arbitrary code. HP has released an advisory to address the vulnerabilities.

Description:

Multiple critical vulnerabilities have been identified with HP 3PAR Service Processor (SP) running OpenSSL and Bash. The vulnerabilities reported are as follows:

- The OpenSSL vulnerability known as “Heartbleed” and this could be exploited remotely disclose information.

- The SSLv3 vulnerability known as “Padding Oracle on Downgraded Legacy Encryption” also known as “Poodle”, which could be exploited remotely resulting in disclosure of information.

- The Bash Shell vulnerability known as “Shellshock” and could be exploited remotely resulting in execution of code.

Solution

HP has released the following software updates to resolve the above vulnerabilities in HP 3PAR Service Processor (SP) and they are:

- HP 3PAR Service Processor SP-4.1.0.GA-97.P011
- HP 3PAR Service Processor SP-4.2.0.GA-29.P003
- HP 3PAR Service Processor SP-4.3.0.GA-17.P001

More information about the updates is available on:

https://h20564.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c04595094

Vendor Information

Hewlett Packard
www.hp.com

CVE Information

CVE-2014-0224

CVE-2014-3566

CVE-2014-6271

CVE-2014-7169

References

HP Support Centre
https://h20564.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c04595094

HP 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