National Computer Board

Computer Emergency Response Team of Mauritius (CERT-MU)

Targeted Security Alert

TA-2015-09

HP StoreEver MSL6480 Tape Library running OpenSSL, Remote Code Execution

Original Issue Date: March 2015

Severity Rating: High

Potential Security Impact: Remote execution of code

Software Affected:

- HP StoreEver MSL6480 Tape Library firmware versions prior to v4.60

Overview:

A critical vulnerability has been identified with HP StoreEver MSL6480 Tape Library running Bash. The vulnerability is known as "Shellshock" and can be exploited remotely to cause execution of arbitrary code.

Description:

A critical vulnerability has been reported in HP StoreEver MSL6480 Tape Library running Bash. The vulnerability is the Bash Shell vulnerability also known as "Shellshock", which could be exploited by remote attackers for remote code execution. The vulnerability exists because GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment.

Solution

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

- HP StoreEver MSL6480 Tape Library firmware v4.60

More information about the update is available on:

1. Go to http://www.hp.com
2. Click on *"Support"*
3. From the pull-down, select *"Drivers & Downloads"*
4. In the *Find my Product* field, enter *"MSL6480"*
5. Expand the *"HP StoreEver MSL6480 Tape Library"* entry
6. Select *"HP StoreEver MSL6480 Scalable Base Module"*
7. Select *"OS Independent"* for the operating system
8. Expand the *"Firmware – Storage Tape"* entry
9. Download the most recent library firmware file, such as HP_MSL6480_4.60.frm

Vendor Information

Hewlett Packard

www.hp.com

CVE Information

CVE-2014-6271

References

Hewlett Packard

www.hp.com

HP Support Centre

https://h20564.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c04599191

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