National Computer Board

Computer Emergency Response Team of Mauritius

(CERT-MU)

CERT-MU

Targeted Security Alert

Multiple Vulnerabilities in HP Products

Original Issue Date: February 2015

Severity Rating: High

Potential Security Impact: Remote execution of code, Denial of Service (DoS), or other vulnerabilities

Software Affected:

HP-UX B.11.31 running NTP version C.4.2.6.4.0 or previous HP-UX B.11.23 running XNTP version 3.5 or previous

Overview:

Critical security vulnerabilities have been identified with certain HP Networking and H3C switches and routers running Network Time Protocol (NTP).

Description:

Multiple vulnerabilities have been identified with certain HP Networking and H3C switches and routers running NTP. These vulnerabilities could be exploited by remote attackers to allow execution of arbitrary code, disclose information and cause a denial of service condition. The vulnerabilities reported are as follows:

1. **Improper Check for Unusual or Exceptional Conditions**

A vulnerability exists because the length value in extension field pointers is not properly validated and this can result in information leaks.

2. **Insufficient Entropy in Pseudo-Random Number Generator (PRNG)**

A vulnerability exists if no authentication key is defined in the *ntp.conf* file and this causes a cryptographically-weak default key to be generated.

3. **Use of Cryptographically Weak PRNG**

This vulnerability exists because the *ntp-keygen* before 4.2.7p230 uses a non-cryptographic random number generator with a weak seed to generate symmetric keys.

4. **Stack Buffer Overflow**

This vulnerability can allow a remote unauthenticated attacker to craft special packets that trigger buffer overflows in the ntpd functions *crypto_recv()* (when using autokey authentication), *ctl_putdata()*, and *configure()*. The resulting buffer overflows may be exploited by remote attackers to allow arbitrary malicious code to be executed with the privilege of the *ntpd* process.

5. **Error Conditions, Return Values, Status Codes**

This vulnerability exists because a section of code in *ntpd* handling a rare error misses a return statement which causes processing not to stop when the error is encountered. This situation may be exploitable by an attacker. The NTP Project implementation is widely used in operating system distributions and network products. These vulnerabilities affect *ntpd* acting as a server or client.

Solution

HP has provided the following patch for HP-UX B.11.31. A workaround for HP-UX B.11.23 and B.11.11 to temporarily resolve the vulnerabilities are listed below:

1. A patch for HP-UX B.11.31 is available from:
ftp://ntp42650:Secure12@h2.usa.hp.com
https://h20392.www2.hp.com/portal/swdepot/displayProductInfo.do?productNumber=HPUX-NTP

2. Mitigation steps for HP-UX B.11.23 and B.11.11 for CVE-2014-9295:
Restrict query for server status (Time Service is not affected) from *ntpq/ntpdc* by enabling *.noquery*. using the restrict command in */etc/ntp.conf file.*

Vendor Information

Hewlett Packard

www.hp.com

CVE Information

CVE-2014-9293

CVE-2014-9294

CVE-2014-9295

CVE-2014-9296

CVE-2014-9297

References

HP Support Centre

https://h20564.www2.hp.com/hpsc/doc/public/display?docId=emr_na-c04574882

NTP Security Notice

http://support.ntp.org/bin/view/Main/SecurityNotice

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