CERT-MU Advisory

CERT-MU

CERT-MU AD-2016-04

MULTIPLE VULNERABILITIES AFFECTING IBM SECURITY NETWORK PROTECTION

Original Issue Date: 24 August 2016

Severity Rating: High

Overview:

Multiple vulnerabilities have been identified affecting IBM Security Network Protection. These vulnerabilities could be exploited by remote / local attackers to traverse directories, gain elevated privileges, execute arbitrary commands, cause denial of service condition, cause buffer overflow, bypass security restrictions and obtain potentially sensitive information on the target system. IBM has issued updates and remediation(s) to addresses these vulnerabilities.

Description:

Multiple vulnerabilities have been identified affecting IBM Security Network Protection. These vulnerabilities could be exploited by remote / local attackers to traverse directories, gain elevated privileges, execute arbitrary commands, cause denial of service condition, cause buffer overflow, bypass security restrictions and obtain potentially sensitive information on the target system.

The vulnerabilities reported are as follows:

- Multiple vulnerabilities in file affecting IBM Security Network Protection:
    - A vulnerability exists in Fine Free file. This vulnerability is caused by the failure to properly restrict the amount of data read during a regex search. This vulnerability could be exploited by remote attackers using a specially-crafted file to consume all available CPU resources.

- A vulnerability exists in PHP. This vulnerability is caused by an incomplete fix related to the cdf_read_property_info() function. This vulnerability could be exploited by remote attackers to cause the application to crash.

- A vulnerability exists in PHP. This vulnerability is caused by an out-of-bounds read in the donote() function. This vulnerability could be exploited by remote attackers by persuading a victim to open a specially-crafted elf file. Causing the executable to crash.

- A vulnerability exists in file(1). This vulnerability is caused by an error in the readelf.c file. This vulnerability could be exploited by remote attackers to cause a denial of service.

- A vulnerability exists in file(1). This vulnerability is caused by an error in the softmagic.c file. This vulnerability could be exploited by remote attackers to cause a denial of service.

- A vulnerability exists in file. This vulnerability is caused by an error in the in the ELF parser. This vulnerability could be exploited by remote attackers to cause a denial of service using an overly long string.

- A vulnerability exists in file. This vulnerability is caused by an out-of-bounds read in readelf.c. This vulnerability could be exploited by remote attackers by persuading a victim to open a specially-crafted elf file, to cause a denial of service or to execute arbitrary code on the system.

- Multiple Vulnerabilities in Network Time Protocol (NTP) affecting IBM Security Network Protection:

  - A vulnerability exists in ntp_crypto.c. This vulnerability could be exploited by attackers using a packet containing an extension field with an invalid value for the length of its value field to cause ntpd to crash.

  - A vulnerability exists in CRYPTO_ASSOC. This vulnerability is caused by caused by a memory leak in CRYPTO_ASSOC. This vulnerability could be exploited by remote attackers to obtain sensitive information.

  - A vulnerability is caused by an uninitialized variable when processing malicious commands. This vulnerability could be exploited by remote attackers by sending a specially crafted logconfig configuration command causing the daemon to crash.

- A vulnerability exists because of an error in the sntp program. This vulnerability could be exploited by remote attackers by sending specially crafted NTP packets, causing the application to enter into an infinite loop.

- A vulnerability exists because of an error in in ntp_crypto.c. This vulnerability could be exploited by remote attackers using a packet containing an extension field with an invalid value for the length of its value field to cause ntpd to crash.

- A vulnerability exists because of a NULL pointer dereference. This vulnerability could be exploited by remote attackers by sending a specially crafted ntpdc reslist command causing a segmentation fault.

- More vulnerabilities in NTP can be found at http://www-01.ibm.com/support/docview.wss?uid=swg21985122&myns=swgother&mynp=OCSSHLHV&mync=E&cm_sp=swgother-_-OCSSHLHV-_-E

- Multiple Vulnerabilities in OpenSSL affecting IBM Security Network Protection:

  - A vulnerability exists because of a memory error in the BIO_*printf() functions. This vulnerability could be exploited by attackers to trigger an out-of-bounds read using specially crafted data.

  - A vulnerability exists because of improper bounds checking by the EVP_EncodeUpdate() function. This vulnerability could be exploited by remote attackers by sending an overly long argument causing a buffer overflow and execution of arbitrary code on the system or cause the application to crash.

  - A vulnerability exists because of an error when the connection uses an AES CBC cipher and the server support AES-NI. This vulnerability could be exploited by remote attackers to conduct a man-in-the-middle attack via the POODLE (Padding Oracle On Downgraded Legacy Encryption) attack to decrypt traffic.

  - A vulnerability exists because of a buffer underflow when deserializing untrusted ASN.1 structures. This vulnerability could be exploited by an attacker to corrupt memory and trigger an out-of-bounds write and execute arbitrary code on the system.

- More vulnerabilities in OpenSSL can be found at http://www-01.ibm.com/support/docview.wss?uid=swg21984583&myns=swgother&mynp=OCSSHLHV&mync=E&cm_sp=swgother-_-OCSSHLHV-_-E

- Multiple Vulnerabilities in libxml2 affecting IBM Security Network Protection:
  - A vulnerability exists because of a memory corruption error in libxml2. This vulnerability could be exploited by an attacker by persuading a victim to open a specially-crafted XML file.
  - A vulnerability exists because of a format string error. This vulnerability could be exploited by an attacker by using a specially crafted html file containing malicious format specifiers.
  - A vulnerability exists because of a XML external entity (XXE) error when processing XML data by the XML parser. This vulnerability could be exploited by a remote attacker to obtain sensitive information.
  - A vulnerability exists because of an error in the xmlStringGetNodeList() function when parsing xml files while in recover modeThis vulnerability could be exploited by a remote attacker to obtain sensitive information.
  - More vulnerabilities in libxml2 affecting can be found at http://www-01.ibm.com/support/docview.wss?uid=swg21986974&myns=swgother&mynp=OCSSHLHV&mync=E&cm_sp=swgother-_-OCSSHLHV-_-E

- Multiple Vulnerabilities in OpenSSH affecting IBM Security Network Protection:
  - A vulnerability exists because of an error when making connections after ForwardX11Timeout expired. This vulnerability could be exploited by an attacker to bypass XSECURITY if X11 connections are forwarded with ForwardX11Trusted=no.
  - A vulnerability exists because of the acceptance of extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests by the monitor component in sshd. This vulnerability could be exploited by an attacker to conduct impersonation attacks
  - A vulnerability exists because of a use-after-free error in the mm_answer_pam_free_ctx function. This vulnerability could be exploited by a local attacker to gain elevated privileges on the system.

Impact of the attack(s)

A remote / local attacker can:

- traverse directories
- gain elevated privileges
- execute arbitrary commands
- cause memory corruption
- cause denial of service condition
- cause buffer overflow
- bypass security restrictions and
- obtain potentially sensitive information on the target system

Affected System:

- IBM Security Network Protection 5.3.1
- IBM Security Network Protection 5.3.2

CVE Information:

CVE-2014-3538	CVE-2014-3587	CVE-2014-3710	CVE-2014-8116	CVE-2014-8117
CVE-2014-9620	CVE-2014-9653	CVE-2015-7691	CVE-2015-7692	CVE-2015-7701
CVE-2015-5194	CVE-2015-5195	CVE-2015-5219	CVE-2015-7702	CVE-2015-7703
CVE-2015-7852	CVE-2015-7977	CVE-2015-7978	CVE-2015-7979	CVE-2016-1547
CVE-2016-1548	CVE-2016-1550	CVE-2016-2518	CVE-2016-0799	CVE-2016-2105
CVE-2016-2106	CVE-2016-2107	CVE-2016-2108	CVE-2016-2109	CVE-2016-2842
CVE-2016-1762	CVE-2016-1833	CVE-2016-1834	CVE-2016-1835	CVE-2016-1836
CVE-2016-1837	CVE-2016-1838	CVE-2016-4448	CVE-2016-4449	CVE-2016-1839
CVE-2016-1840	CVE-2016-3627	CVE-2016-3705	CVE-2016-4447	CVE-2015-5352
CVE-2015-6563	CVE-2015-6564			

Solution

Users are advised to apply updates.
More information about the updates is available on:

http://www-01.ibm.com/support/docview.wss?uid=swg21985753&myns=swgother&mynp=OCSSHLHV&mync=E&cm_sp=swgother-_-OCSSHLHV-_-E

http://www-01.ibm.com/support/docview.wss?uid=swg21985122&myns=swgother&mynp=OCSSHLHV&mync=E&cm_sp=swgother-_-OCSSHLHV-_-E

http://www-01.ibm.com/support/docview.wss?uid=swg21984583&myns=swgother&mynp=OCSSHLHV&mync=E&cm_sp=swgother-_-OCSSHLHV-_-E

http://www-01.ibm.com/support/docview.wss?uid=swg21986974&myns=swgother&mynp=OCSSHLHV&mync=E&cm_sp=swgother-_-OCSSHLHV-_-E

http://www-01.ibm.com/support/docview.wss?uid=swg21987978&myns=swgother&mynp=OCSSHLHV&mync=E&cm_sp=swgother-_-OCSSHLHV-_-E

References:

IBM

http://www-01.ibm.com/support/docview.wss?uid=swg21985753&myns=swgother&mynp=OCSSHLHV&mync=E&cm_sp=swgother-_-OCSSHLHV-_-E

http://www-01.ibm.com/support/docview.wss?uid=swg21985122&myns=swgother&mynp=OCSSHLHV&mync=E&cm_sp=swgother-_-OCSSHLHV-_-E

http://www-01.ibm.com/support/docview.wss?uid=swg21984583&myns=swgother&mynp=OCSSHLHV&mync=E&cm_sp=swgother-_-OCSSHLHV-_-E

http://www-01.ibm.com/support/docview.wss?uid=swg21986974&myns=swgother&mynp=OCSSHLHV&mync=E&cm_sp=swgother-_-OCSSHLHV-_-E

http://www-01.ibm.com/support/docview.wss?uid=swg21987978&myns=swgother&mynp=OCSSHLHV&mync=E&cm_sp=swgother-_-OCSSHLHV-_-E

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. Please note that the members who do not want to receive the security alert, can unsubscribe from CERT-MU mailing list by sending an e-mail to the following address: unsubscribe@cert.ncb.mu

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: http://cert-mu.org.mu