Primera 存储针对 CVE-2011-1473 漏洞扫描问题

存储系统 孔樱【技术大咖】 2022-05-18 发表

组网及说明

某运营商通过绿盟扫描，发现Primera存在 CVE-2011-1473 漏洞问题，希望我司解决。该漏洞描述：** DISPUTED ** OpenSSL before 0.9.8l, and 0.9.8m through 1.x, does not properly restrict client-initiated renegotiation within the SSL and TLS protocols, which might make it easier for remote attackers to cause a denial of service (CPU consumption) by performing many renegotiations within a single connection, a different vulnerability than CVE-2011-5094. NOTE: it can also be argued that it is the responsibility of server deployments, not a security library, to prevent or limit renegotiation when it is inappropriate within a specific environment.

Generic protocol issue, no code fix. Workarounds exist, see bug #672456
and http://vincent.bernat.im/en/blog/2011-ssl-dos-mitigation.html

问题描述

该问题是如果存储开启了Openssl重协商功能，会有可能导致存储 CPU 资源耗尽的潜在风险。
只要关闭了OpenSSL重协商功能问题就可以规避。

过程分析

```
[root@pikefc cinder(keystone_admin)]# openssl s_client -connect 10.12.172.76:443 -tls1_2
CONNECTED(00000003)
depth=0 CN = HP_3PAR_CN701503MQ
verify error:num=18:self signed certificate
verify return:1
depth=0 CN = HP_3PAR_CN701503MQ
verify return:1
---
Certificate chain
0 s:/CN=HP_3PAR_CN701503MQ
   i:/CN=HP_3PAR_CN701503MQ
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIDCjCCAfKgAwIBAgIBADANBgkqhkiG9w0BAQsFADAdMRswGQYDVQQDDBJIUF8z
UEFSX0NONzAxNTAzTVEwHhcNMjIwMTA4MDM0MTM5WhcNMzIwMTA2MDM0MTM5WjAd
MRswGQYDVQQDDBJIUF8zUEFSX0NONzAxNTAzTVEwggEiMA0GCSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQDU7DcIgRr5Ej3MaetA74v+x9xz4u7ul/0A55rHilp93nWY
jCZNryrhOcDS/0IGOpu0zHM651a1N80lfYJSGBfDMWt2HtvO0OxoeNyGk85Kb5Rx
euWbFDi0/5Rea8u4IhNpAwhIsPuDui623Omc29RQeyDsPQS+AJ2kjxzsLfV4+hr+
mnADGV5zMkRGvDvgQ9La824wYvL8bsHnliZS8Lh4cUA5XKT3WQKCD2KOjiDGrZKL
y9yhbvtLydQSSg2msY6+yaWMOY72YZZsIk7mYkXQMrL00WRAD+jZODw9x0PDBVtM
3I8zJ1BY3WIv+U9GH2mR9yNiDjshI57rYP5PH6fjAgMBAAGjVTBTMBMGA1UdJQQM
MAoGCCsGAQUFBwMBMB0GA1UdDgQWBBRuXlwlk1H9x0IRRFIZmu/5+9ddKDAdBgNV
HREEFjAUghJIUF8zUEFSX0NONzAxNTAzTVEwDQYJKoZIhvcNAQELBQADggEBADfD
axBZXWEUD5l/T6ED+7W6MMd3fpvxl4/3m3WOnlBf35Yv8muwonL00mUkr2r5AjyR
ao0TmQWyRK+21L4aH+EeZPf2btkLqNWdDiD+QQMUEDXx5BvR/+R2ipJrSy75TaXj
on1I+j5e6QvZ8lMbPJOUdW6rHxSyE/jjiagG1dud1sm4cOmx/FoL3V8pFd06YRyY
mA9E4RVT8UoKp6NLfdeyrtYGNW6OAnZwyNv4sSQYyP94uHcuKNwdca15av43ldCL
NKgMhSG1+HpuRZEs1xN7shxxB/a53KEO+3A1p/5peAVnfQ11V0LD3+w1ZytdmA1D
m/Jt4antWYDoOc9OiyU=
-----END CERTIFICATE-----
subject=/CN=HP_3PAR_CN701503MQ
issuer=/CN=HP_3PAR_CN701503MQ
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits
---
SSL handshake has read 1403 bytes and written 415 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
    Session-ID: BBC26EFB755A681F192B989601152A22F46268DFE3FFE42D7D149F61B3FEBFC9
    Session-ID-ctx:
    Master-Key: C3D178A4CCC5526B78424DC3829975A969EF4D9715A6BCC907B37EB7651742FE99E15F2B0CC0B87135
CD70677975C70D
    Key-Arg   : None
    Krb5 Principal: None
    PSK identity: None
    PSK identity hint: None
    TLS session ticket:
    0000 - f1 c7 24 e9 73 bc 47 e3-c8 60 db a8 9e b1 5f dd   ..$.s.G..`...._.
    0010 - 2d df 88 60 55 52 b1 d6-f8 89 68 8a 37 8c 4e e5   -..`UR....h.7.N.
    0020 - ba 4b b1 f7 37 94 0b 72-31 c8 8d da f5 0f 51 36   .K..7..r1.....Q6
    0030 - b6 bb 2b 9f c1 91 ae cc-e7 23 87 22 9a cf 82 e3   ..+......#."....
    0040 - 48 69 9a 0c b2 9a 4c 07-68 c9 13 78 f7 5c 34 26   Hi....L.h..x.\4&
    0050 - 38 9c f4 13 29 ce 96 df-4c 8b 4b 14 8c d3 8b 1c   8...)...L.K.....
    0060 - 22 3d a9 4b bb f2 d1 43-c8 9a 49 d9 3d 34 04 ef   "=.K...C..I.=4..
    0070 - f4 ae b0 11 26 22 d2 78-37 07 43 31 74 6b 9d 74   ....&".x7.C1tk.t
    0080 - af                                                .

    Start Time: 1652211089
    Timeout   : 7200 (sec)
    Verify return code: 18 (self signed certificate)
---
R              >>>> 输入 R (Re-negotiation)
RENEGOTIATING
139917452371872:error:140943F2:SSL routines:ssl3_read_bytes:sslv3 alert unexpected message:s3_pkt.c:1493:SSL alert nu
mber 10
139917452371872:error:1409E0E5:SSL routines:ssl3_write_bytes:ssl handshake failure:s3_pkt.c:659:
[root@pikefc cinder(keystone_admin)]#
```

解决方法

找一台Linux服务器，执行命令 : openssl s_client -connect xx.xx.xx.xx:443 可以验证是否开启 OpenSSL 重协商功能。