Suricata - Security #3169

tls: out of bounds read (5.x)

09/17/2019 09:47 AM - Victor Julien

Status: Closed
Priority: Normal
Assignee: Victor Julien
Category: Target version: 5.0rc1
Affected Versions: 5.0beta1
CVE: 2019-15699
Git IDs: 922f4f7d78055ed96833b43cb0c086fe37

tls: out of bounds read (5.x)
09/17/2019 09:47 AM - Victor Julien

Status: Closed
Priority: Normal
Assignee: Victor Julien
Category: Target version: 5.0rc1
Affected Versions: 5.0beta1
CVE: 2019-15699
Git IDs: 922f4f7d78055ed96833b43cb0c086fe37

Description

==7789==ERROR: AddressSanitizer: heap-buffer-overflow on address 0x6060000031d6 at pc 0x555555dec3b7 bp 0x7fffffff8530 sp 0x7fffffff8528
READ of size 1 at 0x6060000031d6 thread T0
0x555555dec3b6 in TLSDecodeHSHelloExtensionSupportedVersions /home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/src/app-layer-ssl.c:962:42
1 0x555555de8b1b in TLSDecodeHSHelloExtensions /home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/src/app-layer-ssl.c:1224:23
2 0x555555de33d3 in TLSDecodeHandshakeHello /home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/src/app-layer-ssl.c:1353:11
3 0x555555dd4eb in SSLv3ParseHandshakeType /home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/src/app-layer-ssl.c
4 0x555555dd9d903c in SSLv3ParseHandshakeProtocol /home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/src/app-layer-ssl.c:1620:14
5 0x555555dcb3b2 in SSLv3Decode /home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/src/app-layer-ssl.c:2293:22
6 0x555555dc3402 in SSLDecode /home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/src/app-layer-ssl.c:2471:30
7 0x555555d41f6 in AppLayerParserParse /home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/src/app-layer-parser.c:1188:13
8 0x555555d51d98 in LLVMFuzzerTestOneInput /home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/fuzzing/playground/app_ssl/fuzz_app_ssl.c:103:3
9 0x555555e1e3832 in fuzzer::Fuzzer::ExecuteCallback(unsigned char const*, unsigned long) (/home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/fuzzing/playground/app_ssl/fuzz_app_ssl+0x178f832)
10 0x555555e4d3da4 in fuzzer::RunOneTest(fuzzer::Fuzzer*, char const*, unsigned long) (/home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/fuzzing/playground/app_ssl/fuzz_app_ssl+0x178f832)
11 0x555555eedcace in fuzzer::FuzzerDriver(int*, char**, int (*)(unsigned char const*, unsigned long)) (/home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/fuzzing/playground/app_ssl/fuzz_app_ssl+0x178f0e)
12 0x555555e4d3d23 in main (/home/sirko/Projects/CI/fuzzing/._CPP/suricata/suricata-fuzzing.4.1.4/fuzzing/playground/app_ssl/fuzz_app_ssl+0x178f0e)

Related issues:
Copied from Security #3168: tls: out of bounds read

History

#1 - 09/17/2019 09:47 AM - Victor Julien
- Copied from Security #3168: tls: out of bounds read added

#2 - 09/24/2019 02:51 PM - Victor Julien
- Status changed from Assigned to Closed
- Priority changed from High to Normal
- Private changed from Yes to No

https://github.com/OISF/suricata/commit/922f4f7d78055ed96833b43cb0c086f37e2b672

#3 - 09/01/2020 09:07 AM - Victor Julien
- Tracker changed from Bug to Security
- CVE set to 2019-15699
- Git IDs updated