HERCULES SecDevice Release Note

Release Version: 2025r1.01
Release Date: 2025/02/27
System version: v1.4.5115

- Features:
  - Add authentication mechanisms functionality confirmation for SSH (OnSec-TC-05011001)
- Enhancement:
  - More CVEs support.
- Bug fixed:
  - Fixed the ineffective test case (OnSec-TC-03011005 OpenSSH User Enumeration) caused by using the wrong version of the Paramiko library.
  - Fixed the issue where SecDevice did not wait long enough for the DUT to reboot.
  - Fixed the issue in the Wi-Fi WPS key crack test case, where the DUT was ignored if it did not send vendor information in the beacon packet.

Release Version: 2024r4.01-Hoxfixed
Release Date: 2025/01/06
System version: v1.4.5108

- Optimization:
  - Refine the core of fuzzer module to prevent took too much time when error pattern locating after DUT crash.
- Bug fixed:
  - Fixed that didn't wait enough time after reboot DUT reboot when the power switch module connected.
  - Fixed the syntax error in OSPF and RIP fuzzer module.
  - Fixed the fuzzer module can't recognize correct network interface issue.

Release Version: 2024r4.01
Release Date: 2024/11/27
System version: v1.4.5107

- Enhancement:
  - Enhanced Wi-Fi WPS Key crack testcase (OnSec-TC-04003001).
  - Unified the timeout value of fuzzing testcases to 180 seconds, to prevent false alert due to the unstable or build-in firewall of DUT.
    - ◆ OnSec-TC-01003012   IPv6 TCP Fuzz Testing
    - ◆ OnSec-TC-01003013   IPv6 UDP Fuzz Testing
    - ◆ OnSec-TC-01003014   IPv6 ICMP Fuzz Testing
    - ◆ OnSec-TC-01003015   IPv6 Fuzz Testing
    - ◆ OnSec-TC-01004001   EDSA IPv4 Fuzz Testing
    - ◆ OnSec-TC-01004002   EDSA IPv4 TCP Fuzz Testing
    - ◆ OnSec-TC-01004003   EDSA IPv4 UDP Fuzz Testing
    - ◆ OnSec-TC-01004004   EDSA IPv4 ICMP Fuzz Testing
    - ◆ OnSec-TC-01005001   IEC61850 MMS Fuzz Testing

- OnSec-TC-01005002   IEC61850 GOOSE Fuzz Testing
- OnSec-TC-01005003   IEC61850 SV Fuzz Testing
- OnSec-TC-01005008   GOOSE Certification Testing
- OnSec-TC-01008001   IGMPv3 Query Fuzz Testing
- OnSec-TC-01008002   IGMPv3 Report Fuzz Testing
- OnSec-TC-01008003   OSPFv2 Fuzz Testing
- OnSec-TC-01008004   RIPv2 Fuzz Testing
- OnSec-TC-01008005   LLDP Fuzz Testing
- OnSec-TC-01009001   EDSA ARP Fuzz Testing
- OnSec-TC-01010001   EDSA Ethernet Fuzz Testing
- OnSec-TC-03002006   HTTP Fuzz Testing
- OnSec-TC-03003006   TLSv1.2 Server Fuzz Testing
- OnSec-TC-03003007   TLSv1.3 Server Fuzz Testing
- OnSec-TC-03004002   UPnP Fuzz Testing
- OnSec-TC-03005004   NETBIOS-SSN Fuzz Testing
- OnSec-TC-03006004   NTP Server Fuzz Testing
- OnSec-TC-03007002   RTSP Fuzz Testing
- OnSec-TC-03007003   ONVIF Fuzz Testing
- OnSec-TC-03008002   FTP Fuzz Testing
- OnSec-TC-03010009   DNS Server Fuzz Testing
- OnSec-TC-03010010   DNS Server Zone Transfer Fuzz Testing
- OnSec-TC-03011006   SSH Fuzz Testing
- OnSec-TC-03013002   Telnet Server Fuzz Testing
- OnSec-TC-03015001   RTCP Fuzz Testing
- OnSec-TC-03016001   SNMPv3 Fuzz Testing
- OnSec-TC-03016002   SNMPv1 Fuzz Testing
- OnSec-TC-03016003   SNMPv2 Fuzz Testing
- OnSec-TC-03016004   SNMPv1 Trap Fuzz Testing
- OnSec-TC-03016005   PPTP Fuzz Testing
- OnSec-TC-03017001   OPCUA Fuzz Testing
- OnSec-TC-03018001   IEC104 Fuzz Testing
- OnSec-TC-03019001   DNP3 TCP Fuzz Testing
- OnSec-TC-03019002   DNP3 UDP Fuzz Testing
- OnSec-TC-03020001   RTP Fuzz Testing
- OnSec-TC-03021001   Modbus TCP Fuzz Testing
- OnSec-TC-03022001   DHCPv4 Server Fuzz Testing
- OnSec-TC-03022002   DHCPv6 Server TCP Fuzz Testing
- OnSec-TC-03023001   EtherNet/IP Messaging Fuzz Testing
- OnSec-TC-03024001   BACnet Fuzz Testing
- OnSec-TC-03025002   Profinet Fuzz Testing
- OnSec-TC-03027001   TFTP Server Fuzz Testing
- OnSec-TC-03028001   LDAPv3 Server Fuzz Testing
- OnSec-TC-03029001   CoAP Server Fuzz Testing
- OnSec-TC-03030001   OCSP Server Fuzz Testing
- OnSec-TC-03031001   SIP UAS Fuzz Testing
- OnSec-TC-03032001   CWMP (TR69) ACS Fuzz Testing
- OnSec-TC-03033001   BGP Server Fuzz Testing

- ◆ OnSec-TC-03033002   BFD Server Fuzz Testing
- ◆ OnSec-TC-03034001   RADIUS Server Fuzz Testing
- ◆ OnSec-TC-03034002   RADIUS Server Accounting Fuzz Testing
- ◆ OnSec-TC-03035001   IKEv2 Server Fuzz Testing
- ◆ OnSec-TC-03036001   IPMI Server Fuzz Testing
- ◆ OnSec-TC-03037001   FINS Server Fuzz Testing
- ◆ OnSec-TC-03038001   NFSv4 Server Fuzz Testing
- ◆ OnSec-TC-03039001   VLAN Server Fuzz Testing
- ◆ OnSec-TC-03040001   S7comm Server Fuzz Testing
- ◆ OnSec-TC-03041001   IPsec Fuzz Testing
- ◆ OnSec-TC-03044001   DICOM Fuzz Testing
- ◆ OnSec-TC-03044002   MQTT Fuzz Testing
- ◆ OnSec-TC-03044003   CIP Fuzz Testing
- ◆ OnSec-TC-03044004   HL7v2 Fuzz Testing
- ◆ OnSec-TC-03044005   HL7v3 CDAr2 Fuzz Testing
- ◆ OnSec-TC-03044006   HL7v3 FHIR Fuzz Testing
- **Bug fixed:**
  - Fixed the abnormal function of check button when create new web target in Website Configuration page.

Release Version: 2024r3.01
Release Date: 2024/09/27
System version: v1.4.5074
- **Features:**
  - Update Machine-id to identify the version.
- **Enhancement:**
  - More CVEs supports.
  - Update CVE automation flow and structure for latest test items.
  - Update the result validation for EDSA test case.
  - Update the frontend DEKRA Logo.
- **Bug fixed:**
  - Fix Vlan test case Pre-check packet mechanism(OnSec-TC-03039001).

Release Version: 2024r2.02
Release Date: 2024/06/17
System version: v1.4.5038
- **Features:**
  - Add Wi-Fi WPA3 client mode fuzz testing (OnSec-TC-04005005)
  - Add Wi-Fi WPA3 AP mode fuzz testing (OnSec-TC-04005006)
- **Enhancement:**
  - More CVEs supports.
  - Update when loop enable remain time change to loop time countdown.
  -
- **Bug fixed:**
  - Remove the problematic characters in HL7v3 FHIR fuzzing policy.
  - Remove the skip and loop frontend interfaces in the WF module.

- Remove the skip and loop frontend interfaces in the WA module.

Release Version: 2024r2.01
Release Date: 2024/05/17
System version: v1.4.5019
● Features:
  - Add a test case for HL7 CDAR2
  - Add a test case for HL7 FHIR
  - Add a test case for TLS1.3
  - Remove the AI Fuzz Testing test case
● Enhancement:
  - More CVEs supports.
  - Modify log message about skip and loop function
● Bug fixed:
  - Fix the nmap issue
  - Fix jlog bug and loop error
  - Remove unnecessary logs and Fix crash caused by excessive logging

----

Release Version: 2024r1.01
Release Date: 2024/03/07
System version: v1.4.4900
● Features:
  - None
● Enhancement:
  - More CVEs supports.
● Bug fixed:
  - Fix add_report bug.

Release Version: 2023r2.01
Release Date: 2023/07/04
System version: v1.4.4882
● Features:
  - None
● Enhancement:
  - More CVEs supports.
  - Enhance the testing with the Juniper Routers as DUTs of the TestCase: RIPv2 Fuzz Testing.
  - Loose the waiting time, when a WiFi client tries to connect to SecDevice.
● Bug fixed:
  - Fix an eternity loop bug about the TestCase: Known Vulnerability Testing.

Release Version: 2023r1.01
Release Date: 2023/03/24
System version: v1.4.4816
● Features:
  - None

- **Enhancement:**
  - More CVEs supports.
  - Loose the check timing of the TestCase: RTSP Fuzz Testing.
  - Loose the check timing of the TestCase: OSPFv2 Fuzz Testing.
  - Loose the check timing of the TestCase: RIPv2 Fuzz Testing.
- **Bug fixed:**
  - Fix a PowerSwitch control problem, while the SecDevice is doing a fuzzing backward test.

Release Version: 2022r4.01
Release Date: 2022/12/20
System version: v1.4.4762
- **Enhancement:**
  - More CVEs supports.

Release Version: 2022r3.01
Release Date: 2022/10/04
System version: v1.4.4762
- **Enhancement:**
  - More CVEs supports.
- **Bug fixed:**
  - SecDeviece log Front-end layout adjustment

Release Version: 2022r2.01
Release Date: 2022/06/30
System version: v1.4.4758
- **Features:**
  - Support HL7 Analysis.
  - Support GeoIP Testcase.
  - Support Profinet TestCase.
- **Enhancement:**
  - More CVEs supports.
  - Loose the check timing of the TestCase: EDSA ARP Translation Cache Flood.
  - Enhance auto ip detection.
  - Enhance UDP Fuzzing mechanism.
- **Bug fixed:**
  - Fix databaselock on boot.
  - Fix ja_JP locale translation.
  - Fix firmware uploading failed issues.
  - Fix export issues.
  - Fix Web Assessment bug.

Release Version: 2021r4.01
Release Date: 2021/11/18
System version: v1.4.4661
- **Features:**

- Support source IP Geolocation Analysis.
- Support ONVIF Protocol Fuzz Testing.
● Enhancement:
- Enhanced Command Injection judgment mechanism, add padding data for determine.
● Bug fixed:
- Fixed Known Vulnerability Testing always restart issue.
- Fixed main website could not startup normally issue.
- Fixed Network Configuration setting issue.
- Fixed IPsec Fuzz Testing (Policy 04) occurred error issue.
- Fixed DNS Server Fuzz Testing parsing packet detail error issue.
- Fixed Fuzz Testing occurred wrong number of pattern issue.
- Fixed UDP Fuzz Testing testcase occurred system crash.

Release Version: 2021r3.01
Release Date: 2021/8/3
System version: v1.4.4352
● Features:
  - Support fuzzing new protocol- OSPFv2 (Routing protocol)
  - Mapping test case into OWASP IOT top 10
    Support
      ■ I1: Weak, Guessable, or Hardcoded Passwords
      ■ I2: Insecure Network Services
      ■ I3: Insecure Ecosystem Interfaces
      ■ I4: Use of Insecure or Outdated Components
      ■ I7: Insecure Data Transfer and Storage
    User can get OWASP IOT top 10 PDF report
● Enhancement:
  - Html report now will show every targets host information if every target's testcase are pass.
  - Html report now will show every targets host information even if some target's testcase are failed.
  - General PDF report will show every targets host information if every target's testcase are pass.
● Bug fixed:
  - Fixed manual crawling web can't work normally in some conditions
  - known vulnerability can't not run issue.

Release Version: 2021r2.02
Release Date: 2021/5/26
System Version: v1.4.4300
● Features:
  - New version of PDF report(Support OWASP web top 10)
● Enhancements:
  - FW upload support larger than 2 GB of FW size(VM version)
  - SSL/TLS Weak Cipher Algorithm testcase substitute by SSL/TLS service category (25 testcases)

- Bug fixed:
  - Known vulnerability scan result parse error(VM version)
  - Fixed some security vulnerability

Release Version: 2021r2.01
Release Date: 2021/5/6
System Version: v1.4.4267
- Enhancements:
  - Packet Information support for all protocol fuzzing testcase
  - known vulnerabilities scan engine upgrade, improve scan availability.
  - Following protocol fuzzing pattern up to 100000
    - MMS,GOOSE,SV,DNP3,Ethernet,IPv4,TCP, UDP,ICMP ,ARP
- Bug fixed:
  - OnSec-TC-04003001 WPS Crack Testing N/A (VM version)

Release Version: 2021r1.02
Release Date: 2021/3/22
System Version: v1.4.4192
- Features:
  - provide 1 ssl testcase
    - blowfish algorithm testing
- Enhancements:
  - modbus fuzzing testing
    - up to 500,000 fuzzing pattern
- Bug fixed:
  - portlist problem

Release Version: 2021r1.01
Release Date: 2021/2/22
System Version: v1.4.4137
- Features
  - Support CIP protocol fuzz testing
  - Provide 2 of SSH Security test cases:
    - RC2, RC4 Algorithm Testing
    - Provide 12 of HTTPS Security test case.
    - RC2, RC4 Algorithm Testing
    - DES,3DES
    - Key Length of Asymmetric and Symmetric Algorithm Testing
    - DROWN
    - Lucky Thirteen Attack (LUCKY13)
    - ROBOT
    - SSL 64-bit Block Size Cipher Suites Supported (SWEET32)
    - IDEA, CBC Mode Algorithm Testing
- Enhancements
  - improve WiFi testing coverage
    - client fuzz new policy：

- ◆ Deauthentication
- ◆ Disassociation
  - ■ wpa client fuzz new policy:
    - ◆ Deauthentication
  - ■ ap fuzz new policy：a
    - ◆ Reassociation Request
  - ■ wpa ap fuzz new policy：
    - ◆ Reassociation Request
    - ◆ User can setup specified vlan id for VLAN Fuzz testing
    - ◆ Packet Information support fuzz protocol
    - ◆ Ipv6_tcp, ipv6_udp, ipv6_icmp, mms, goose, sv, dnp3_tcp, dnp3_udp, modbus_tcp, edsa_arp, edsa_icmp

----

Release Version: 2020r3.04
Release Date: 2020/12/23
System Version: v1.3.0.3998
- ● Features
  - - Provide more coverage of HTTPS Security test case:
    - ■ Check two weak cipher Twofish algorithm and HMAC algorithm
    - ■ Browser Exploit Against SSL/TLS Attack (BEAST)
    - ■ Logjam
- ● Enhancements
  - - Support all protocol fuzzing speed adjustment
  - - More CVE supports

Release Version: 2020r3.03
Release Date: 2020/11/18
System Version: v1.3.0.3958

- ● Features
  - - Provide user-defined options to failure condition in the following test cases:
    - ■ TCP-SYN Scan
    - ■ UDP Port Scan
    - ■ TCP-FIN Scan
  - - Provide new test cases in the following test cases:
    - ■ DICOM Fuzz Testing
    - ■ MQTT Fuzz Testing
  - - Auto Detect functional structure adjustment.

Release Version: 2020r3.02
Release Date: 2020/10/21
System Version: v1.3.0.

- ● Features
  - - Provide Grouping function to All Fuzzing test cases.
  - - More coverage of HTTP Fuzzing test case.

- Add Error locate function to all Fuzzing test cases.
- Enhance TLSv1.2 Server Fuzz Testing to support stateful testing.
- Enhance All Pages Cross Site Request Forgery (CSRF) test cases to support user define tokens.

Release Version: 2020r3.01
Release Date: 2020/09/23
System Version: v1.3.0.3895

● Features
  - Provide new testcases and enhanced testcases:
    ■ Certificate Signing Algorithm
    ■ FREAK
    ■ POODLE
    ■ TLSv1/SSLv3 Renegotiation Vulnerability
    ■ Transport Layer Security (TLS) Protocol CRIME
  - Provide enhanced testcases:
    ■ Heartbleed
    ■ ChangeCipherSpec Injection
  - Provide fuzzing pattern grouping function in the following test cases:
    ■ DHCPv4 Server Fuzz Testing
    ■ DHCPv6 Server Fuzz Testing
    ■ DNS Server Fuzz Testing
    ■ DNS Server Zone Transfer Fuzz Testing
    ■ NTP Server Fuzz Testing
    ■ IPv6 Fuzz Testing
    ■ IPv6 ICMP Fuzz Testing
    ■ VLAN Fuzz Testing
    ■ IGMPv3 Query Fuzz Testing
    ■ IGMPv3 Report Fuzz Testing
    ■ UPnP Fuzz Testing
    ■ FTP Fuzz Testing
    ■ TFTP Server Fuzz Testing
    ■ SNMPv1 Fuzz Testing
    ■ SNMPv1 Trap Fuzz Testing
    ■ EDSA Ethernet Fuzz Testing
    ■ EDSA IPv4 ICMP Fuzz Testing
    ■ EDSA IPv4 UDP Fuzz Testing
    ■ EDSA IPv4 TCP Fuzz Testing
    ■ IPv6 UDP Fuzz Testing
    ■ IPv6 TCP Fuzz Testing
    ■ HTTP Fuzz Testing
    ■ SSH Fuzz Testing
    ■ EDSA ARP Fuzz Testing
    ■ EDSA IPv4 Fuzz Testing
    ■ SNMPv2 Fuzz Testing
    ■ SNMPv3 Fuzz Testing
    ■ Telnet Server Fuzz Testing

- - - - CoAP Server Fuzz Testing
- - - - IPsec Fuzz Testing
- - - - IPMI Server Fuzz Testing
- - - - IKEv2 Server Fuzz Testing
- - - - FINS Server Fuzz Testing
- - - - BGP Server Fuzz Testing
- - - - BFD Server Fuzz Testing
- - - - SIP UAS Fuzz Testing
- - - - SV Fuzz Testing
- - - - OPCUA Fuzz Testing
- - - - OCSP Server Fuzz Testing
- - - - LDAPv3 Server Fuzz Testing
- - - - IEC104 Fuzz Testing
- - - - GOOSE Fuzz Testing
- - - - EtherNet/IP Messaging Fuzz Testing
- - - - DNP3 TCP Fuzz Testing
- - - - DNP3 UDP Fuzz Testing
- - - - CWMP (TR69) ACS Fuzz Testing
- - - - BACnet Fuzz Testing

- **Fixed Issues**
  - Fix Known Vulnerability Testing can not update database issue.

Release Version: 2020r2.04
Release Date: 2020/08/26
System Version: v1.3.0.3786

- **Features**
  - Provide new testcases:
    - SSLv2 Testing
    - SSLv3 Testing
    - TLSv1.0 Testing
    - TLSv1.1 Testing
  - Provide fuzzing pattern grouping function in the following test cases:
    - CoAP Server Fuzz Testing
    - DHCPv4 Server Fuzz Testing
    - EDSA ARP Fuzz Testing
    - EDSA Ethernet Fuzz Testing
    - EDSA IPv4 TCP Fuzz Testing
    - EDSA IPv4 UDP Fuzz Testing
    - EDSA IPv4 ICMP Fuzz Testing
    - HTTP Fuzz Testing
    - IPv6 TCP Fuzz Testing
    - IPv6 UDP Fuzz Testing
    - SSH Fuzz Testing
    - SNMPv2 Fuzz Testing
    - SNMPv3 Fuzz Testing
    - Modbus TCP Fuzz Testing
    - Telnet Server Fuzz Testing

- Fixed Issues
  - Optimize the testcase Known Vulnerability Testing to improve test efficiency.
  - Optimize the performance and fault tolerance of WEB Page Account Testing.
  - Enhance checking functions in the following test cases:
    - EDSA IPv4 TCP Fuzz Testing
    - EDSA IPv4 UDP Fuzz Testing
    - DHCPv4 Server Fuzz Testing

Release Version: 2020r2.03
Release Date: 2020/07/29
System Version: v1.3.0.3672

- Features
  - The website test can use the target domain name or IP address.
  - It should not in the test if the specific function of the target is disabled. Add the pre-check mechanism in the following test cases:
    - EDSA IPv4 Fragment Reassembly Flood
    - EDSA IPv4 Raw NPDU Flood
    - EDSA IPv4 Auto-Negotiating Raw NPDU Flood
    - EDSA ICMPv4 Flood
    - EDSA ICMPv4 Auto-Negotiating Flood

Release Version: 2020r2.02
Release Date: 2020/07/01
System Version: v1.3.0.3575

- Security Issues
  - Disable SSL and TLS 1.0 protocol on the Web server.
  - Disable Weak Ciphers on the Web server.
  - Known security issues fixed.
- Fixed Issues
  - It cannot modify the PASS/FAIL result of the testcase, OnSec-TC-03014001 Known Vulnerability Testing.
  - Fix an issue that the General Setting page cannot reopen.

Release Version: 2020r2.01
Release Date: 2020/06/03
System Version: v1.3.0.3540

- Features
  - Optimize the user interface for select hosts of multiple targets vulnerability assessments. Increase the maximum number of targets is limited to 64.
- Fixed Issues
  - Improve the performance of access to the fuzz packet information.
  - Fix several issues that had unexpected errors when stop auto crawling.

Release Version: 2020r1.03
Release Date: 2020/04/24
System Version: v1.3.0.3430

- Features
  - Provide new testcase, AI Traffic Capture Fuzz Testing
  - Integrate the fuzzing testcases into SecDevice
    - RADIUS Server Fuzz Testing
    - RADIUS Server Accounting Fuzz Testing
    - VLAN Fuzz Testing
    - BGP Fuzz Testing
    - IPMI Server Fuzz Testing
    - IKEv2 Server Fuzz Testing
    - FINS Server Fuzz Testing
    - NFSv4 Server Fuzz Testing
    - S7Comm Fuzz Testing
    - IPsec Fuzz Testing
    - BFD Server Fuzz Testing
  - Support 802.11 WLAN/WPA AP and WPA client fuzz testing
  - Enhance 802.11 WLAN Client fuzz testing
  - Provide new features in IP Camera related fuzzing testcases
    - related fuzzing testcases:
      - RTP Fuzz Testing
      - RTCP Fuzz Testing
      - RTSP Fuzz Testing
      - TLSv1.2 Fuzz Testing
      - 802.11 WLAN AP Fuzz Testing
      - 802.11 WPA AP Fuzz Testing
      - 802.11 WLAN Client Fuzz Testing
      - 802.11 WPA Client Fuzz Testing
    - features:
  - packet analyzer function
      - fuzzing pattern grouping function
      - sufficient test information
      - user-defined test weight setting in the following fuzzing Information
      - sequential and random test modes
- Fixed Issues
  - Correct the judgment logic of testcase, OnSec-TC-02005001 Cookie Attribute
  - Correct the judgment logic when the device under test reboot

----

Release Version: 2020r1.02
Release Date: 2020/03/11
System Version: v1.3.0.2897

- Features
  - Support the scenario of multiple targets vulnerability assessments.
- Change logs
  - Modify the determining mechanism in testcase SSH Buffer Overflow Testing

(OnSec-TC-03011004)
- Fixed Issues
  - Fix occasional incorrect testing duration information issue.
  - Fix an issue that could not be successfully updated when uploading a new version of SecDevice FW using the webpage.
  - Fix an issue where some files had unexpected errors when crawling.

Release Version: 2020r1.01
Release Date: 2020/02/04
System Version: v1.3.0.2834

- Features
  - IPv4 UDP Fuzz Testing packet analysis function is supported.
  - Provided Traffic collecting function in Wi-Fi module.
- Fixed issues
  - Fix IPv6 UDP Fuzz Testing issues.
  - Suppress the chance of traffic collecting issues.