ONWARD SECURITY
SECURE YOUR OWN WORLD !

MORE THAN A FUZZER

HERCULES SecDevice

Connected Product Security Test Tool

HERCULES SecDevice is a security assessment tool designed for connected products, and provides automated features from test environment configuration to security assessment. Test targets include web and wireless security. The content covers known and unknown security vulnerabilities, as well as user friendly design to help users to quickly get started. Most common vulnerabilities listed in OWASP TOP 10 and SANS TOP 25 are also covered. Onward research team provides quick test project updates to ensure coverage of the latest security issues.

TEST TARGETS

SecDevice uses both known and unknown vulnerabilities testing techniques, and performs black-box testing on the device, targeting the following:

Network: Uses IPv4 or IPv6-based addressing technology. Test packets are sent over the network to a target. The wide test coverage includes device system, drivers, applications, etc.

Web page: URL-based target definition. Many devices do not provide convenient operating method aside from web interface. Since the services are provided through web application, a lot of security issues may appear due to its flexible design, hence web application must be analyzed more thoroughly.

Wireless: Defines test target based on service set identifier (SSID), analyze wireless connectivity service of devices.

KEY FEATURES

Focus on product security: Designed for connected product security testing. As a black Box testing solution, no source code is needed. Automates product security analysis, provide re-testing feature for continuous testing needs.

Portable design: A software & hardware integrated solution that requires no installation. It just needs to be connected to DUT and it is ready to perform. The light weight design allows it to be conveniently used in different labs, and requires no internet connection.

Various testing methods: Uses fuzzing technique, network vulnerability check, web vulnerability scanning, and DoS to find both known and unknown vulnerabilities, including the ones in operating system, web applications, network protocols, webpages and wireless.

Reproducible: Combined with vulnerability database, simultaneously gather data and packets during test, the product also provides related information, sites, and description of the problems to reproduce and solve the issues swiftly.

Update to get the latest vulnerabilities information: Through our dedicated research team, we focus on the latest issues and provide timely test cases updates to shorten response time and minimize the enterprise security risks.

ONWARD SECURITY
+886-2-8911-5035
+886-2-8911-5036
www.onwardsecurity.com
product@onwardsecurity.com

SUPPORTED PROTOCOLS

CORE NETWORK
ARP, ETHERNET, ICMP(v4/v6), IGMPv3, IP(v4/v6), TCP(v4/v6), UDP(v4/v6)

FILE SYSTEMS
CIFS/SMB

ICS/SCADA
BACnet, CoAP, DNP3, EtherNet/IP, IEC 60870-5-104, IEC 61850(Goose/MMS/Sampled Value), Modbus, OPC UA, ProfitNet

NETWORK MANAGEMENT
CWMP, DHCP(v4/v6), DNS, LDAPv3, NTP, OCSP, PPTP, SIP, SNMP(v1/v2/v3/trap), SSHv2, TFTP, Telnet, TLS 1.2, UPnP

WEB APPLICATION
WEB Fuzz(Including XML and JSON format)

VoIP/IMS
RTCP, RTP, RTSP

Wireless
Wi-Fi Client Fuzz

TESTING METHODS

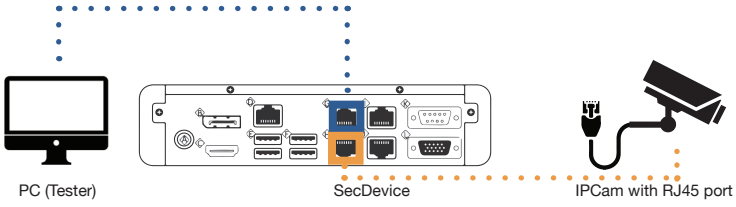
	DESCRIPTION	ADVANTAGES
KNOWN VULNERABILITY	Uses more than 30k test cases from security vulnerabilities database that we continuously update to provide the latest attack methods	Uses the dynamic testing method to check device's status, combined with the environment recognition ability. SecDevice sends probe packets, to accurately uncover any presence of common vulnerabilities.
UNKNOWN VULNERABILITY	Employs intelligent fuzzing test. Generates and sends malformed packets according to different protocols and test regulations, which verifies if the test target contain errors or faults that lead to exploitable vulnerabilities.	Targets various network protocols, automatically generates probe packets. Through modelling of screening mechanism, SecDevice is able to extensively explore potential product security issues using the smallest attack packets.
SECURITY ASSESSMENT	Implements penetration test to find out any security issues. The safety of the device under test can be automatically assessed using programmatic analytical algorithm to evaluate the confidentiality, integrity, and availability of information security.	SecDevice can be used in different testing environment. Its adjustable and dynamic testing mechanism allows flexibility while maintaining accuracy.

SUPPORTED STANDARDS

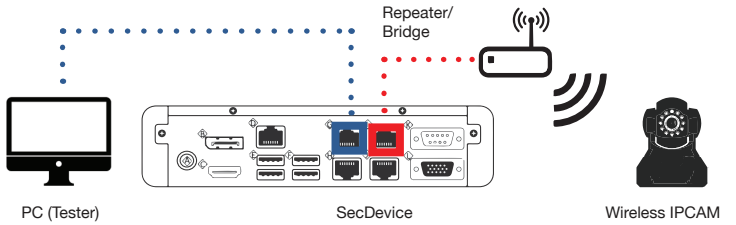
OWASP Top 10 2017
A1 Injection
A2 Broken Authentication
A3 Sensitive Data Exposure
A4 XML External Entities (XXE)
A5 Broken Access Control
A6 Security Misconfiguration
A7 Cross-Site Scripting (XSS)
A8 Insecure Deserialization
A9 Using Components with Known Vulnerabilities

影像監控系統資安標準之測試規範 - 網路攝影機
系統安全測試 - 作業系統安全與網路服務安全測試
系統安全測試 - 網路服務連接埠管控測試
系統安全測試 - 網頁管理介面安全測試
通訊安全測試 - 網路介面通訊協定的安全設置測試
通訊安全測試 - 通訊協定安全測試 （**RTP, RTCP, RTSP, HTTP, TLS)**

TYPICAL DEPLOYMENT



DEVICES WITH SINGLE ETHERNET INTERFACE



DEVICES WITH WIRELESS INTERFACE

ONWARD SECURITY

Onward Security is the leader in connected product security assessment, providing vendors with solutions in every step of product development process to minimize issues, and to comply with standards and regulations. Our team has worked with the government and industry to research and develop security testing and technology.
Onward Security lab possess the capability to uncover zero day. We are committed to the research in the security of IoT, industrial control, and automotive. Onward has won many international awards such as (ISC)² Asia-Pacific ISLA™ and certifications such as ECSA and GPEN.

ONWARD SECURITY
+886-2-8911-5035
+886-2-8911-5036
www.onwardsecurity.com
product@onwardsecurity.com