Security Testing Summary of Next-Generation Enterprise VoIP Solution: Unify Inc. OpenScape SBC V8

SR140531D

19 August 2014

Miercom

www.miercom.com

Overview

Unify Inc. (formerly Siemens Enterprise Communications) engaged Miercom to perform a comprehensive security assessment of a key component of its OpenScape solution portfolio, OpenScape Session Border Controller V8.

The purpose of testing was to attempt to uncover security vulnerabilities that could be exploited to detract from proper, normal operation.

About OpenScape Session Border Controller

V8 is the latest edition of OpenScape SBC, which extends the SIP-based communications and applications of an OpenScape Voice-over-Internet Protocol (VoIP) enterprise network beyond its physical boundary.

OpenScape SBC performs three functions, providing:

- Secure termination of SIP-based trunking from a service provider
- Secure voice communications for remote workers
- A connection to each remote branch office in a distributed OpenScape voice deployment

Unlike traditional data firewall solutions, OpenScape SBC is specifically designed to provide VoIP traffic security.

After terminating a SIP session on its WAN side, outside of the enterprise voice network, OpenScape SBC ensures the traffic is originating from an authorized source and inspects the SIP and media packets for protocol violations or irregularities. Only when the traffic is deemed valid is it passed from the core or LAN side of OpenScape SBC to the OpenScape VoIP enterprise network.

OpenScape SBC also enhances security on the end-user network by providing SIP-aware functionality including dynamic Real-time Transport Protocol/Secure Real-time Transport Protocol pin-holing through its internal firewall, stateful SIP protocol validation, Denial of Service (DoS)/Distributed Denial of Service (DDoS) mitigation, and network topology hiding. It also supports Transport Layer Security encryption on core- and access-side SIP signaling interfaces as well as SRTP media encryption on a termination/mediation or pass-through basis.

Key Findings and Conclusions

- OpenScape Session Border Controller V8 was tested against 10,800,231 attacks and protocol mutations launched by state-of-the-art security tools and Miercom scripts
- An attacker is not able to circumvent the Intrusion Detection System by using a slow rate of traffic to achieve a false login via a brute-force attack
- Exhibited no vulnerability to the Heartbleed exploit as well as a full range of SIP penetration attacks
- Maintained normal operation and call functionality while blocking attempted exploits

Test Conditions

The test environment mirrored an OpenScape voice deployment typical of a mid-sized to large organization that included OpenScape Branch V8 and OpenScape SBC V8. The viability of each attack and the risk of OpenScape SBC being compromised were evaluated.

Copyright © 2014 Miercom

The presence of a compromised computer on the enterprise network, such as one that has been taken over by a botnet, was simulated. State-of-the-art test tools send attacks directly against OpenScape SBC V8. For defense, OpenScape SBC V8 had only its internal firewall. A network security appliance was not present between OpenScape SBC V8 and the attack sources.

"OpenScape Session Border Controller (SBC) proved resilient to a wide range of threats, including five types of SIP attacks and an IPv4 DoS attack."

~ Miercom

The methodology for and the execution of the attacks were based on knowledge Miercom has amassed, in collaboration with leading security experts, from decades of work in VoIP deployments as well as security assessments.

Unify OpenStage 60/80 SIP phones were utilized in the test environment for call up-time verification.

Test Tools Used for Attacks and Vulnerability Scans

Nessus from Tenable Network Security

Spirent Studio Security Software on Spirent Mu-8000 appliance

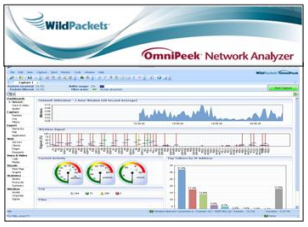
Netcat from Hobbit

Hydra from The Hacker's Choice

Traffic IQ Professional from idappcom

Nmap from nmap.org

Burp Suite from Portswigger Ltd.



OmniPeek from WildPackets

Kali Linux from Offensive Software

back|track Linux

Source: Miercom, August 2014

Two scanners, **Nessus** from Tenable Network Security and **Nmap** from nmap.org, scanned OpenScape SBC V8 to determine what vulnerabilities were present. An active network/host scanner, Nmap provides additional functionality via customized scripts. During this assessment, scripts for SIP attacks, service identification and service fingerprinting were utilized.

Spirent Studio Security software generated protocol mutations, many known (published) vulnerabilities and external attacks using test cases and custom scripts. It was housed on a Spirent Mu-8000 appliance.

Burp Suite from Portswigger Ltd. is an integrated platform for security testing of Web applications. Tools in the suite work together to support the entire testing process, from initial mapping and analysis of the attack surface to sending attacks to exploit security vulnerabilities. Tools include an intercepting proxy, which enables inspection and modification of traffic between the browser and application, and an intruder, which launches customized attacks.

Netcat from Hobbit was used to primarily for service fingerprinting. Also known as the hacker's Swiss Army knife, Netcat creates a socket to any open services.

OmniPeek from WildPackets is a network analyzer that provided Miercom visibility into the test environment.

Hydra from The Hacker's Choice was used in brute-force testing. A password cracker, Hydra launches a dictionary attack to test for weak or simple passwords on one or many remote hosts running a variety of services.

Kali Linux from Offensive Security was utilized to determine that OpenScape SBC V8 is not vulnerable to the Heartbleed exploit. An evolution of back|track Linux, Kali Linux has more than 300 penetration testing and security auditing programs.

Traffic IQ Professional from idappcom Ltd. can be used for a variety of security, audit and compliance tests. In this assessment, it was used for application penetration testing.

back|track Linux is an auditing operating system and toolkit for penetration testing.

Results

OpenScape SBC V8 passed 19 tests in the comprehensive security evaluation, which included vulnerability scans, protocol mutation attacks, SIP attacks and DoS attack. It also passed four additional tests, the highlight of which was validation of resilience to the Heartbleed exploit.

"OpenScape SBC V8 withstood vulnerability scans from the Nmap and Nessus tools and was impervious to all protocol-mutation attacks."

~ Miercom

Snapshot of Security Tests Passed by OpenScape Session Border Controller V8

Category	Action, Assault, Attack	Result
Vulnerability Scans	Metasploit attacks	**Pass**
	Nmap scan of SBC node interfaces	**Pass**
	Nmap scan of SIP signaling interfaces	**Pass**
	Nmap scan of Virtual IP (VIP) ports	**Pass**
	Nessus scan of Virtual IP (VIP) ports	**Pass**
Protocol Mutation Attacks	SNMP mutation	**Pass**
	ICMPv4 mutation	**Pass**
	IPv4 mutation	**Pass**
	ARP mutation	**Pass**
DoS Attack	IPv4 DoS	**Pass**
SIP Attacks	Invite flooding	**Pass**
	Call spoofing	**Pass**
	Enumerating SIP users	**Pass**
	Deregistering SIP users/devices	**Pass**
	Brute force SIP attacks	**Pass**
Other	Heartbleed SSL	**Pass**
	Port scanning and enumeration	**Pass**
	Fragmented attacks (including teardrop, overlapping and tiny fragments)	**Pass**
	Independent local survivability	**Pass**

Source: Miercom, August 2014

Conclusion

Security is crucial for OpenScape Session Border Controller V8 since it operates at a crucial location, the border of an OpenScape VoIP enterprise network.

Based on its strong performance in our comprehensive, hands-on security evaluation, OpenScape SBC V8 is up to the task of securely extending the SIP communications and applications of the VoIP network to SIP service providers, remote branch offices and remote users.

OpenScape SBC V8 demonstrated the ability to sustain call processing functions while subjected to a variety of attacks and exploits from our state-of-the-art test tools.

Unify's OpenScape Session Border Controller V8 has earned **Miercom Certified Secure**.

About Miercom

Founded in 1988, Miercom pioneered the business of independent, hands-on testing of products and services for the enterprise network and communications industry. For over 26 years the company has provided test services and consulting and is considered a leading independent test facility.

Private test services include competitive product analyses as well as individual product evaluations. Miercom features comprehensive certification and test programs including: **Performance Verified**, **Certified Secure**, **Certified Green** and **Certified Reliable**. These certifications are recognized by networking vendors and end-user organizations as an accurate, unbiased validation of the ability of the product or service to perform in a real-world network.

Miercom has published hundreds of network-product-comparison analyses in leading trade periodicals and other publications. For more information about Miercom testing and certifications as well as consulting services, please visit www.miercom.com.