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

SR140532C

19 August 2014

Miercom

www.miercom.com

Overview

Unify Inc. (formerly Siemens Enterprise Communications) engaged Miercom to perform a comprehensive security assessment of OpenScape Voice V8, the latest version of its next-generation enterprise Voice-over-Internet Protocol (VoIP) solution.

The purpose of testing was to attempt to uncover security vulnerabilities that could be exploited to detract from proper, normal operation. This included seeking to gain surreptitious access to place unauthorized calls and to compromise or intercept VoIP communications presumed to be secure.

Also, the resilience exhibited by OpenScape Voice V8 was compared to that of other IP PBX and unified communications (UC) solutions tested previously by Miercom.

About OpenScape Voice

Always part of a solution, OpenScape Voice can function as a stand-alone voice application in basic implementations or with other unified communications (UC) applications in advanced implementations.

A native SIP-based, real-time VoIP system, OpenScape Voice can be deployed in a virtualized architecture and can be delivered as a virtual appliance. Deployment can be on-premise, in a data center as a private cloud by large enterprise customers or as a multi-hosted tenant/public cloud solution by telecommunications service providers.

Massive scalability is among the key attributes of OpenScape Voice. A single system can support up to 100,000 users. But that is not the full extent of scalability. Multiple systems can be networked.

OpenScape Voice provides carrier-grade reliability, meeting or exceeding the “five nines.” The system provides 100% call failover even if the server nodes are geographically separated. If a single node fails, OpenScape Voice will continue to support 100% of the call load. This functionality also enables end-user organizations to reduce the cost and time necessary to implement a disaster recovery strategy.

Also, OpenScape Voice has security functionality, which was challenged in hands-on testing. It includes support for Secure Real-Time Transport Protocol (SRTP) for media encryption and use of Transport Layer Security (TLS) for protecting signaling communications on SIP endpoint, SIP server and SIP-Q server interfaces.

Key Findings and Conclusions

- OpenScape Voice V8 was tested against 10,800,231 attacks and protocol mutations launched by state-of-the-art security tools and Miercom scripts
- The management interface, implemented via the Apache web server, fully blocked all Denial of Service (DoS) attacks (notably Slowloris and THC SSL DoS)
- 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 wide variety of SIP penetration attacks
- Maintained normal operation and call functionality while blocking attempted exploits
- High-availability configuration worked, providing maximum uptime

Test Conditions

OpenScape Voice V8 was tested in a "high availability" configuration. More typical in a higher-end-enterprise deployment, the configuration has contingency measures to maintain call continuity in the event of failure. Each OpenScape Voice server has eight Ethernet ports, two sets of four, which provide fully-redundant network connections.

"The internal countermeasures of OpenScape Voice V8 proved impervious by successfully thwarting a battery of network attacks and vulnerability scans."

~ Miercom

The test environment simulated the presence of a compromised computer on an enterprise network. State-of-the-art test tools send attacks directly against OpenScape Voice V8.

For defense against the attacks, OpenScape Voice V8 had only its internal firewall. A network security appliance was not present between OpenScape Voice V8 and the attack sources.

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.

Test Tools Used for Attacks and Vulnerability Scans

Nessus from Tenable Network Security

Spirent Studio Security Software
on Spirent Mu-8000 appliance

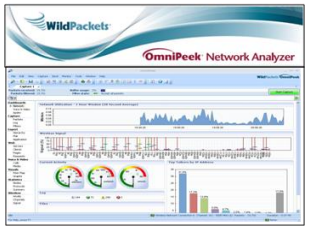
Netcat from Hobbit

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 Voice 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 Voice 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 Voice V8 achieved a perfect score by passing all security tests in the comprehensive program, which consisted of vulnerability scans, protocol mutation attacks, Denial of Service (DoS) attacks, SIP attacks and more.

"OpenScape Voice V8 withstood all 24 attacks from our state-of-the-art tools, brute-force to THC SSL DoS and everything in between."

~ Miercom

Snapshot of Security Tests Passed by OpenScape Voice V8

Category	Action, Assault, Attack	Result
Vulnerability Scans	Metasploit attacks	**Pass**
	Nmap scan of Voice 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	DHCP mutation	**Pass**
	ICMPv4 mutation	**Pass**
	IPv4 mutation	**Pass**
	SIP mutation	**Pass**
DoS Attacks	Slowloris	**Pass**
	THC SSL DoS	**Pass**
	IPv4 DoS	**Pass**
SIP Attacks	SIP Invite flooding	**Pass**
	SIP Call spoofing	**Pass**
	Enumerating SIP users	**Pass**
	Deregistering SIP users/devices	**Pass**
	Brute-force SIP attacks	**Pass**
Other Attacks	Brute-force username/password	**Pass**
	Heartbleed SSL	**Pass**
	Port scanning and enumeration	**Pass**
	Fragmented attacks (including teardrop, overlapping and tiny fragments)	**Pass**
	High Availability of Voice Server	**Pass**

Source: Miercom, June 2014

Conclusion

We were impressed with the flawless performance in comprehensive security testing of OpenScape Voice V8. With only its internal firewall enabled for defense, OpenScape Voice 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.

The performance by OpenScape Voice V8 also raised the bar since it was the best in terms of overall resilience seen to date from any comparable IP PBX or UC solution unified communications product we have tested.

Unify's OpenScape Voice 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.