# Security Testing Summary of Remote Branch Communications: Unify Inc. OpenScape Branch V8

**SR140530C**

**19 August 2014**

**Miercom**

www.miercom.com

## Overview

Unify Inc. (formerly Siemens Enterprise Communications) engaged Miercom to perform a comprehensive security assessment of its OpenScape Branch V8 survivability solution for remote branch communications. The purpose of testing was to ascertain if inherent vulnerabilities exist that an attacker could exploit to:

- Compromise the ability of the system to successfully deliver real-time communications.
- Gain surreptitious access to the system to place unauthorized calls or perform other malicious activity.
- Compromise VoIP communications to monitor, redirect or intercept calls.

## About OpenScape Branch

OpenScape Branch V8 is the latest version of the SIP-based server from Unify that maintains continuity of communications service at a remote branch in the event of WAN link failure between the branch and the home office. It is available on a variety of hardware platforms and as a virtual application. Hardware-based solutions support 24, 48, 80, 250, 500, 1,000 and 6,000 registered lines.

OpenScape Branch includes survivability features, Proxy, Media Server and Session Border Controller. Of the six models of the OpenScape Branch 50i appliance, four provide integrated PSTN Gateway and Analog Terminal Adapter and two provide ATA in higher density. The two models of the 500i provide GW with higher Primary Rate Interface capacity.

OpenScape Branch is a component of OpenScape Voice Solution from Unify. In the test environment, OpenScape Branch in a “branch office” was connected through a switched and routed connection to a “remote” OpenScape Voice system.

If the link between the two servers is lost, OpenScape Branch enters survivability mode to maintain local voice communications. When communication between the servers is restored, OpenScape Branch automatically reverts to full functionality.

## Key Findings and Conclusions

- OpenScape Branch V8 can be configured for standalone survivability, maximizing uptime for users in a remote branch
- The Intrusion Detection System prevents an attacker from using a slow rate of traffic to achieve a false login via a brute-force attack
- OpenScape Branch V8 was tested against 10,800,231 attacks and protocol mutations launched by state-of-the-art security tools and Miercom proprietary scripts
- Maintained normal operation and call functionality while blocking attempted exploits
- Exhibited no vulnerability to the Heartbleed exploit as well as a wide variety of SIP penetration attacks

## Test Conditions

The test environment simulated the presence of a compromised computer on an enterprise network. State-of-the-art test tools sent attacks directly to OpenScape Branch V8, which had only its internal firewall for defense. Unify OpenStage 60/80 SIP phones were utilized for call uptime verification.

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.

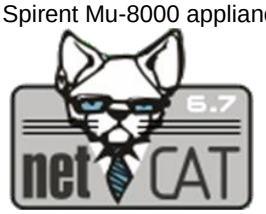
*"OpenScape Branch V8 proved resilient to a wide range of threats, including SIP and protocol-mutation attacks, and most recent exploits using state-of-the-art vulnerability testing tools."*

~ Miercom

## Test Tools Used for Attacks and Vulnerability Scans


Nessus from Tenable Network Security


Spirent Studio Security software on Spirent Mu-8000 appliance



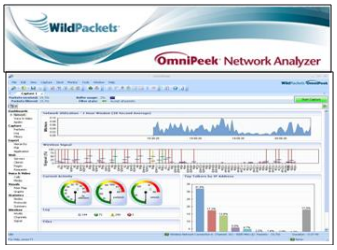

Netcat from Hobbit


Hydra from The Hacker's Choice


Traffic IQ Professional from idappcom Ltd.


Nmap fromnmap.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 Branch 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 provides Miercom comprehensive visibility into the test environment at multiple simultaneous locations.

**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 Branch 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 Branch V8 passed 21 tests in the comprehensive security program as shown below.

*"OpenScape Branch V8 exhibited resiliency against a full range of security threats during hands on testing."*

**~ Miercom**

## Snapshot of Security Tests Passed by OpenScape Branch V8

| Category | Action, Assault, Attack | Result |
|---|---|---|
| Vulnerability Scans | Metasploit attacks | **Pass** |
| | Nmap scan of Branch 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 Attack | IPv4 DoS | **Pass** |
| SIP Attacks | Invite flooding | **Pass** |
| | Call spoofing | **Pass** |
| | Enumerating SIP users | **Pass** |
| | Deregistering SIP users/devices | **Pass** |
| Other Attacks | Brute-force SIP | **Pass** |
| | 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

Miercom was impressed with the ability of OpenScape Branch V8 to protect call-processing functions against a wide range of threats, including vulnerability scans, protocol-mutation attacks and SIP attacks. It also withstood brute-force and fragmented attacks and was impervious to the Heartbleed exploit.

**Unify's OpenScape Branch 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.