Security Assessment Report

OpenScape SBC V9

February 2016

DR151217B

Miercom

www.miercom.com

Contents

1 - Executive Summary

Unify Communications engaged Miercom to perform a thorough, independent security assessment of its latest OpenScape SBC V9, a key component of the OpenScape IP-PBX system. The testing evaluated the inherent security features and countermeasures of OpenScape SBC, with no additional external security gateways or firewalls between the OpenScape SBC and the attack station.

The purpose of the testing was to uncover any evident security vulnerabilities that a scurrilous insider assailant could exploit to disrupt the proper, normal operation of OpenScape SBC. Miercom conducted a similar audit of this system in mid-2014. In this testing some of the previous attacks that had no effect were deleted, and have been replaced with new attacks that have emerged recently.

All exploits on the OpenScape products were launched from an inside source, on the internal network – as noted, with no other security protection between the assailant and the hardened OpenScape system. Tests included a broad and complex set of exploits launched by security tools and scripts to stress and penetrate the OpenScape SBC system.

Overall, the OpenScape products proved more secure than most comparable products we have tested to date, and exhibited effective resilience through multiple batteries of exploit and penetration tests. Our audit resulted in only a few, relatively minor security notes; there was no immediate or severe threat or vulnerability uncovered for a properly configured OpenScape V9 system.

The internal countermeasures built into the firewall of OpenScape SBC were all enabled for testing. The approach and methodology utilized in these tests are based on knowledge that Miercom, in collaboration with leading security experts, has amassed from years of working in VoIP pre- and post-deployment site surveys, as well as security assessments.

This document provides an overview of the results and details of the more noteworthy exploit attempts that were conducted. In a few cases details have been intentionally omitted, so as not to aid in any surreptitious reverse-engineering of the exploits.

The OpenScape SBC products tested were configured in accordance with guidance from Unify Communications, documented in the OpenScape SBC Security Checklist, which we believe effectively enhances the resiliency of these systems.

Key Findings and Conclusions

- OpenScape SBC V9 blocked Denial-of-Service (DoS) attacks. We delivered DoS assaults using HPING3 – including "Ping of Death" at up to 10,000 pings/second – along with attacks from the Spirent Studio and Ixia's BreakingPoint system.
- An attacker is unable to circumvent the IDS (Intrusion Detection System) by using a slow rate of traffic, or achieve access via a brute-force attack (via a false login). We applied a Hydra brute-force attack and learned that system access was solely via SSH (Secure Shell) key-based authentication, which makes penetration by brute-force password attacks impossible.

- OpenScape SBC was resilient to the many thousands of attacks and protocol mutations we launched against it. These were delivered using the latest security programs and in many cases Miercom-proprietary scripts.
- OpenScape SBC was fully protected against any Heartbleed vulnerability, as well as a number of recent exploits, including GHOST, VENOM and the Bash Bug (aka Shellshock). Previous testing, reconfirmed in this audit, concluded that SIP-specific penetration attacks had no effect. Nessus confirmed OpenScape was not vulnerable to such SIP-based attacks, including mutated SIP packets.
- OpenScape SBC V9 maintained normal operation and call functionality while blocking all attempted exploits. In all cases, while attacks were underway, we were able to dial and set-up calls between HQ LAN and Remote-WAN phones, with average call set-up times about 1 second.

The test results are detailed in the following sections of this document. We were impressed with the performance of OpenScape SBC V9 in its demonstrated ability to sustain call processing functions even while undergoing malicious exploits and attacks.

Miercom is pleased to present the Miercom Certified Secure award to OpenScape SBC V9.

Robert Smithers

CEO

Miercom

Summary of OpenScape SBC V9 Security Tests and Results

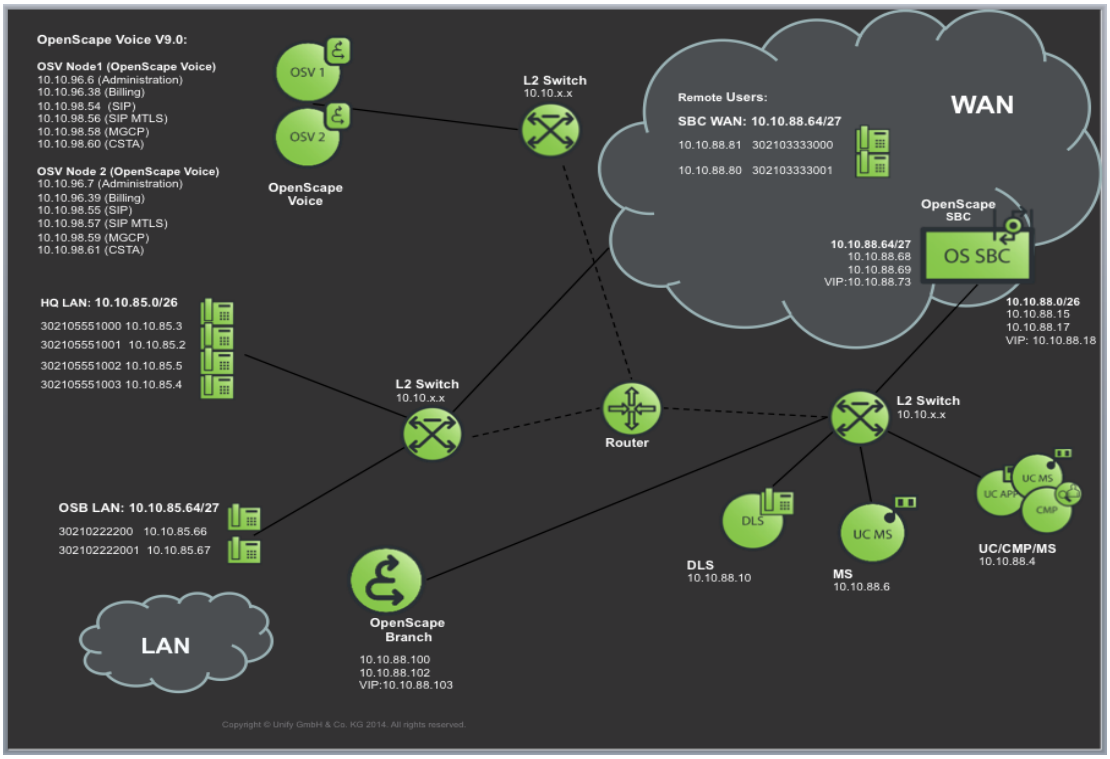
Category	Action, Assault, Attack	Result	See Page
Observations	General security environment	**Pass**	11
	National Vulnerability Database check	**Pass**	11
Vulnerability Scans	Metasploit penetration testing	**Pass**	12
	Nmap scan against all OpenScape SBC node interfaces	**Pass**	12
	Nmap scan against all SIP interfaces, ports and services	**Pass**	13
	Nessus scan of all IP ports	**Pass**	13
	Web vulnerability	**Pass**	13
Protocol-Mutation Attacks	ARP mutation attack	**Pass**	14
	DNS mutation attack	**Pass**	14
	ICMP mutation attack	**Pass**	15
	IPv4 mutation attacks	**Pass**	15
	SIP mutation attacks	**Pass**	16
	TCP mutation attack	**Pass**	16
	RTP mutation attack	**Pass**	17
	UDP mutation attack	**Pass**	17
DoS Attacks	IPv4 and ICMP DoS	**Pass**	18
	TCP and TCP-SYN-flood DoS	**Pass***	18
	UDP and UDP-DNS-flood DoS	**Pass**	20
	ICMP and ICMP-port-unreachable DoS	**Pass**	20
	ARP DoS	**Pass**	20
Other	Published-vulnerability attacks	**Pass**	21
	Deregistering SIP users/devices	**Pass**	21
	Brute force username/password	**Pass**	21
	Protocol Fuzzing attack	**Pass**	22
	Heartbleed SSL attack	**Pass**	22
	Ghost attack	**Pass**	22
	Venom attack	**Pass**	22
	Shellshock (Bash Bug) attack	**Pass**	23

2 - OpenScape SBC V9 Test Bed

A test-bed network, depicted in the diagram below, was set up for the security testing of OpenScape SBC. The OpenScape SBC systems were connected in a dual-node "high availability" configuration. Such a configuration features contingency measures to maintain service availability in case an OpenScape SBC system application fails the SBC nodes run primary and hot failover. The SBC pair is shown at the right of the test-bed diagram below.

The security assessment was conducted directly from an attack source on the HQ LAN to the OpenScape SBC V9 – without any intervening security gateways, firewalls or SBC. This simulated the case where a local laptop, desktop or server was compromised becoming remotely accessible, or bot-controlled or otherwise used to launch malicious attacks against the OpenScape SBC system.

Figure 1: Logical Configuration of OpenScape SBC V9 Test Bed



As the test-bed diagram shows, other key nodes in the OpenScape family – OpenScape Voice and OpenScape Branch – were also included and were also tested as part of this security audit. The results for OpenScape Voice and Branch are detailed in separate reports.

The test environment included various Unify SIP phone models to confirm call processing was unaffected by individual attacks, and verification of normal call set-up time.

The CMP and DLS management stations were specifically not tested or directly attacked as part of this security audit, and neither were any media servers. The OpenScape SBC nodes do not routinely handle VoIP media streams but may, depending on requirements. Media handling is largely relegated to media servers. Our audit did however confirm that all management traffic was sent via TLS-encrypted tunnels, and media streams were encrypted via Secure RTP (SRTP).

3 - How We Did It

More than a dozen tools were employed in this security audit, including Miercom-proprietary attacks and scripts. The software tools used included the following:

- **Ixia's** powerful **BreakingPoint** system was used to generate attack files from its 6,000-attack database.
- **HPING3,** a command-line tool for issuance of high volumes of ICMP messages, such as for Ping Denial-of-Service (DoS) attacks.
- **Hydra**, a brute-force password checking software tool.
- **Kali Linux** 2.0 (released August 2015), an advanced penetration-testing Linux distribution, designed for network security assessments.
- **Metasploit,** a popular open source penetration testing framework from Rapid 7.
- **Nessus,** v6.5.3 (November 2015), vulnerability scanner, from Tenable Network Security.
- **Nikto**, v2.1.6, an open source Web server scanner, runs automatically by SPARTA.
- **NMAP** 7.0 (included as part of Kali Linux 2.0).
- **SPARTA** 1.0.2 beta (released March 2015), a Python GUI application that augments NMAP scanning and enumeration, a "network-infrastructure penetration tool."
- **Spirent's Studio** (formerly Mu Dynamics) vulnerability analysis and attack-generation system was used extensively to produce DoS, protocol-mutation and other attack files.
- **Traffic IQ Professional** v2.2.0, from UK-based **idappcom**, a security audit package capable of generating threat attacks, used in this testing to issue PCAP attack files.
- **Vega**, a Web vulnerability scanner, offered by Subgraph, a Montreal-based security software company.

In addition, the following resources and processes were employed:

- The NIST (National Institute of Standards and Technology) National Vulnerability Database for all vulnerabilities reported in SUSE products since 2014.

- The attacks were launched using Kali Linux 2.0 and Windows 7 in a virtualized environment, provided by Oracle VM Virtual Box, version 5.0.8.

All of these diverse test tools and resources, including customized proprietary test scripts, commercial vulnerability scanning tools, and open-source security assessment products were employed to conduct the tests and produce the results presented in this report.

A VoIP network infrastructure typical of a mid- to large-sized enterprise was simulated to support a conventional OpenScape Voice, OpenScape Branch and OpenScape SBC deployment. The objective of the attacks we launched was to compromise the OpenScape SBC V9 system and to interrupt real-time voice communications.

Initial scanning. NMAP port scanner and Nessus vulnerability scanner were used to probe each system in the OpenScape infrastructure to determine what ports were open, what services were running and what possible vulnerabilities could be exploited.

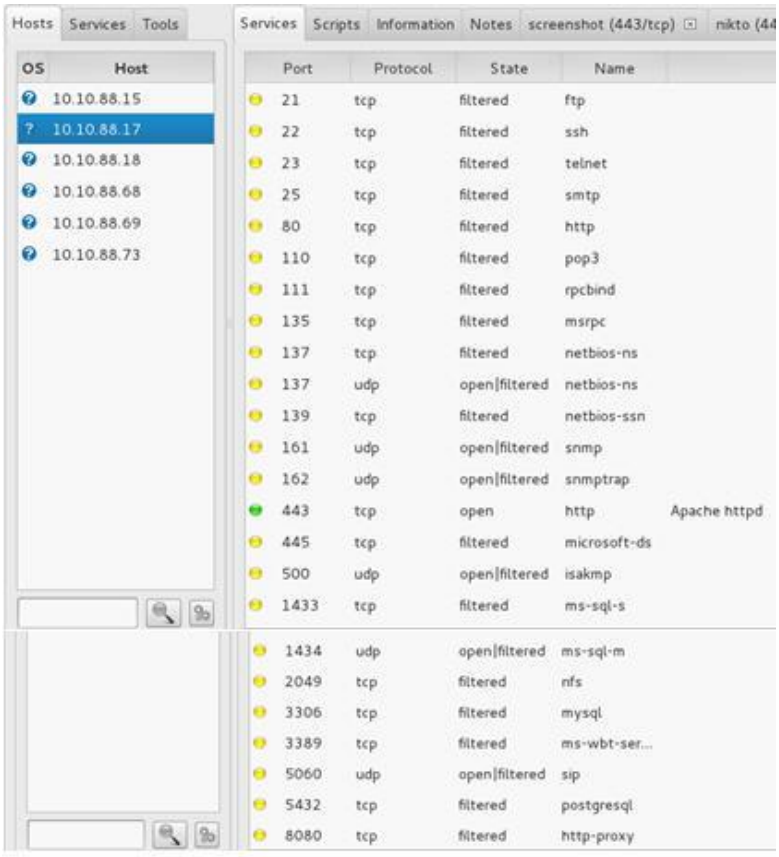
NMAP 7.0 – a part of Kali-Linux-2.0 suite – is the most robust port scanner on the market today, and provides additional functionality via customized scripts. During this assessment several additional NMAP scripts were used – including for SIP attacks, service identification and service fingerprinting.

Nessus is Tenable Network Security's premier vulnerability scanner, widely adopted by penetration testers and other security consultants.

If vulnerabilities are suspected, both scanners generate a short report detailing each vulnerable port. Once open ports have been identified and isolated, attacks are then planned for bombarding the exposed system.

The summary results of the NMAP scan of the dual, redundant OpenScape SBC V9 nodes are detailed in the following screenshots.

NMAP Results: Open, Filtered and Open/Filtered Ports on OpenScape SBC Nodes



Key to NMAP determination (per NMAP documentation):

- **Open**: An application is actively accepting TCP connections, UDP datagrams or SCTP associations on this port. An open port is an avenue for attack, and while open ports are necessary for network operations, these need to be kept to a minimum.
- **Filtered**: Usually probe messages are dropped, but some minimal information is leaked. These ports frustrate attackers because too little useful information is obtained, usually due to firewall filtering. Nmap cannot determine whether the port is open or not.
- **Open/filtered**: NMAP is unable to determine if the port is open or being filtered because the port gives no response to certain probe messages. This can be because a packet filter dropped the probe message and/or the response to it.

The security audit applied many attacks originally created by Spirent Studio Security. This is software housed on a Spirent Mu 8000 appliance. In addition, attacks were applied that were originally generated by an Ixia BreakingPoint system. These tools were used to generate protocol mutations, many known published vulnerabilities, and external attacks using test cases and custom scripts.

The attacks were saved as PCAP files and applied via an idappcom package, Traffic IQ Professional. All of the attacks were individually directed at each IP interface of the devices under test OpenScape Voice, OpenScape Branch and OpenScape SBC.

4 - General Security Environment

4.1 Over-Willingness to Respond to Pings

We observed throughout the audit that our attack station, directly connected on the same LAN as OS SBC, was able to obtain ICMP responses to individual Pings (ICMP requests) regularly, on almost all of OS SBC IP interfaces.

Observations and Analysis – PASS

We originally thought that OS SBC response to pings could be a vulnerability. On investigation we learned that, by design, OS SBC does respond to ping requests from stations on the same LAN interface. This is hard-coded and cannot be disabled. On the WAN side, ping replies are disabled by default, although they can be enabled.

However, we do not believe that responding to ping requests necessarily constitutes an OS SBC vulnerability – because any appreciable volume of pings can be throttled by rate limiting. The rate limiting is settable and very effective. In our testing, OS SBC effectively rate-limited any station sending more than 300 packets per second (pps). We confirmed that our attack station was indeed blocked after sending more than 300 pps as part of our ICMP flood attack.

4.2 National Vulnerability Database Check

The list of packages included in OpenScape Voice, Branch and SBC was checked against the NIST, National Institute of Standards and Technology National Vulnerability Database, for all vulnerabilities reported in SUSE products (including the SBC's OpenSUSE) since 2014.

Observations and Analysis - PASS

We confirmed that Unify is not shipping any vulnerable software packages in any of the OpenScape products we tested.

5 - Vulnerability Scans

5.1 Metasploit Penetration Testing

Description

The Metasploit Project is an open-source computer-security project that provides information about security vulnerabilities, which aids in penetration testing and IDS (intrusion detection system) signature development. One of its well-known sub-projects is the Metasploit Framework, a tool for developing and executing exploit code against a remote target computer. Via Metasploit, 493 discrete attacks were applied. All of these yielded negative results in this security audit.

OpenScape SBC V9 should not be compromised on any level.

Observations and Analysis - PASS

OpenScape SBC deflected or thwarted 100 percent of the penetration attempts on all attempted attack vectors. We were unable to gather any information or detect any vulnerability that would help successfully penetrating the server. The Nmap report revealed that the OpenScape SBC had port 22 or Secure Shell (SSH) partially open filtered.

The primary filtered ports were 22, 23, 53, 443, 2427, 5060, and 5061. Penetration attempts were made on all of these ports to determine if a common exploit was not properly addressed. A total of 493 penetration attacks were attempted on all interfaces combined. No attempts succeeded.

5.2 Nmap Scan against All OpenScape SBC Node Interfaces

Description

An Nmap scan was conducted against all of the OpenScape SBC node interfaces to find port vulnerabilities.

Observations and Analysis - PASS

The Nmap scan revealed that OpenScape SBC node interfaces had ports 22 and 443, as well as ports 23, 53, 2427, 5060, and 5061 filtered, but responsive. Port 22, or SSH is used for secure communication between two network devices. SSH uses an encrypted public-key encryption channel. In this topology, the SSH port on the nodal interfaces may be used for modifying or viewing configurations on the server from a remote location. It is highly unlikely that this open SSH port could be used as an attack entry point. Nor is the open SSH port susceptible to eavesdropping, since the communication channel is encrypted.

All other ports were tested rigorously. Port 443 is used for SSL communication, and ports 5060 and 5061 are SIP signaling interfaces – which were secured using TLS (transport layer security) and authenticated users only. Ports 22, 443, 5060 and 5061 were also operating openly, but successfully filtered all attempts to fingerprint the services running behind them.

5.3 Nmap Scan against all SIP Interfaces, Ports and Services

Description

An Nmap scan was performed against the OpenScape SIP interfaces, ports and services to find vulnerable ports.

Observations and Analysis - PASS

The Nmap software tool could not identify any accessible or open ports. We therefore conclude that the SIP signaling interface on OpenScape SBC V9 is secure. Ports 5060 and 5061 were filtered appropriately, meaning that only authenticated users could communicate to this device over TLS encrypted tunnels.

5.4 Nessus Vulnerability Scan against OpenScape SBC

Preliminary port scans were performed on each system within the scope of the security testing. The most common services running included HTTPS (443), SSH (22) and SIP (5060, 5061). Each service was fingerprinted for specific versions in use and for vulnerability mapping.

Observations and Analysis - PASS

The OpenScape SBC system did not yield any results in response to attempts to obtain the specific version of these services. The operating system **was** identified as Linux, but we were unable to successfully identify the distribution and kernel version, which were protected. This is an important safeguard, since many attacks are effective only against a specific Linux operating system version or service.

5.5 Web Vulnerability

Several scans were run specifically to detect vulnerabilities in Web applications in all the OpenScape nodes with a Web interface available (supporting HTTPS over port 443). In addition, Burp Suite was used for manual investigation and proxy analysis of the Web application. The Web Application scan settings within Nessus and the Vega vulnerability scanner were also applied.

Observations and Analysis – PASS

Vega 1.0, a vulnerability scanner like Nessus, from Subgraph, turned up a possible absolute filesystem path – that is, not related to the Web root – on the OpenScape SBC node. Specifically, the files revealed were: /lib/* -- all files in the /lib/ directory.

On further investigation, we learned that, in the case of OS SBC, the /lib directory contains the JavaScript files that must be read by the browser, and can be reached even without authentication. One method to protect JavaScript is to use Obfuscation, which makes it hard to debug and maintain.

In OS SBC, the Web interface can be restricted to the administrator only.

6 - Protocol-Mutation Attacks

The protocol-mutation attacks used in this security assessment were created using Spirent Studio Security. The attacks tested for vulnerabilities in OpenScape SBC 's protocol implementations, looking for fault responses that might be exploited. The Spirent mutation engine delivers highly specific test cases that are built based on the state, structure and semantics of protocols, as well inter-dependencies with other protocols.

Protocol-mutation attacks incorporate deviations from the expected operation of stateful protocol implementations. Secure and robust targets should handle mutated-protocol packets by dropping them. However, a system with protocol-implementation flaws would respond abnormally, revealing a vector for a more malicious attack.

6.1 ARP Protocol-Mutation Attack

Description

The Address Resolution Protocol (ARP) is a basic, low-level, state-based protocol used to resolve a device's Layer-3 IP address with its associated MAC (Layer-2) address. The Mutated-ARP attack, generated from the Spirent Studio Security, was sent at high volume triggering rate limiting and then at below-rate-limit under 300 pps for OpenScape SBC.

The test was set up to attack at OpenScape SBC interfaces using permutations of ARP request and reply messages.

Observations and Analysis - PASS

The OpenScape SBC completely blocked the attempted attack, launched against every IP address of each OpenScape SBC node individually, as well as the Virtual IP interface. OpenScape SBC completely rejected this attack. No faults were reported. We confirmed that the Mutated-ARP attack had no effect on call set-up between HQ-LAN and OSB-LAN phones)within the 1-second normal time frame, and all call features during the attack attempts remained fully operational.

6.2 DNS Protocol-Mutation Attack

Description

The Domain Name Service (DNS) is a key state-based IP protocol in which, normally, devices query a Domain Name Server to learn a device's Layer-3 IP address. The Mutated-DNS attack, generated from the Spirent Studio Security, was sent at high volume triggering rate limiting and at below-rate-limit rates under 300 pps for OpenScape SBC.

The test was set up to attack at OpenScape SBC interfaces using permutations of the dozens of different DNS messages. The OpenScape SBC should completely block the attempted attack.

Observations and Analysis - PASS

No faults were reported, and we confirmed that the Mutated-DNS attack, launched against every IP address of each OpenScape SBC node individually, had no effect on call set-up within the 1-second normal time frame. OpenScape SBC completely rejected all these attacks. No vulnerabilities in OpenScape SBC were detected and all call features during the attack attempts remained fully operational.

6.3 ICMP Protocol-Mutation Attack

Description

This attack was also generated by Spirent Studio Security from its suite of proprietary protocol-mutation tools. ICMP, essentially a ping, is deployed universally in all IP-based networks. Its main purpose is to monitor the status of a requested service, host or router and determine its availability and connectivity access. It can also be used as a diagnostic or network tracer tool. IP addressing is crucial to ICMP's proper operation, and any corruption of IP address could cause loss of network connectivity, or even failure of the target system.

The test is configured to attack the OpenScape SBC interfaces using ICMPv4 echo requests pings and fragmented mutated echo requests. OpenScape SBC should completely block the attempted attacks and normal operations should continue.

Observations and Analysis - PASS

All attacks were rejected successfully and no faults were reported. OpenScape SBC dropped all mutated packets and did not issue any error messages as a result. No vulnerabilities in the ICMPv4 protocol implementation on the OpenScape system were detected.

The ICMP protocol mutation attack against OpenScape SBC contained 52,155 different variants/attack vectors. These variants were implemented in ICMP echo requests and ICMP fragmented echo request messages.

6.4 IPv4 Protocol-Mutation Attack

Description

This test attacks the OpenScape SBC interfaces using IPv4 datagrams and fragmented datagrams. IP version 4 is a connectionless protocol, typically supporting the Ethernet family of networking technologies for local area networks below it, and higher-layer connection-oriented protocols, such as TCP, for wide-area data transport and end-to-end connectivity above it.

IPv4 works on a best-effort delivery basis. The network-layer IP does not guarantee the delivery of data or a quality of service level. In other words, IP's performance depends to a large degree on the current traffic load. The uniqueness and correctness of IPv4 addresses is key. IP addresses are vulnerable to attack and corruption, and a device with a corrupted IP device can fail. A primary objective of this attack was to corrupt the IP address of the target device.

Observations and Analysis - PASS

All attack attempts were thwarted successfully and no faults were reported. OpenScape SBC dropped all mutated packets, did not report any error messages, and no vulnerabilities in OpenScape SBC IPv4 protocol implementation were detected.

The IPv4 attacks that were run against OpenScape SBC contained 31,129 variants/attack vectors consisting of IPv4 normal, mutated and fragmented datagrams.

6.5 SIP Protocol-Mutation Attacks

Description

This series of attacks attempts to exploit target-system vulnerabilities in handling mutated SIP messages and traffic. SIP messages have been deliberately modified to cause abnormal handling conditions and results.

SIP calls require a source and destination URI (phone number) that the SIP call server uses to establish communication between the calling and called entities. SIP communications can run over TCP or UDP – two very different transport-layer protocols. And more secure SIP communications can be established by using TLS. TCP and UDP commonly use port 5060, while TLS typically uses port 5061.

SIP messages are made up mainly of REGISTER, INVITE, ACK, CANCEL, BYE AND OPTIONS. This attack was configured to attack OpenScape SBC using SIP INVITE-CANCEL messages, and used UDP over port 5060 initially.

Observations and Analysis - PASS

The OpenScape SBC completely blocked the attempted attacks – dropping all malformed SIP packets to and from unregistered users – and continued normal operations. With the default configuration, which forced TLS for all connections, all the attacks, lacking valid credentials, were rejected.

6.6 TCP Protocol-Mutation Attack

Description

The TCP is the fundamental state-based, connection-oriented protocol that is universally implemented in IP networks. It is used primarily to facilitate data exchange and contains many mechanisms to assure that a user's data is conveyed correctly. There are many TCP protocol components and many opportunities to mutate TCP messages.

The Mutated-TCP attack, generated from the Spirent Studio Security, was delivered at high volume triggering rate limiting and at below-the-rate-limit rates under 300 pps for OpenScape SBC.

The test was set up to attack at OpenScape SBC interfaces using hundreds of permutations of TCP messages. The OpenScape SBC should completely block the attempted attack.

Observations and Analysis - PASS

No faults were reported, and we confirmed that the Mutated-TCP attack, launched against every IP address of each OpenScape SBC node individually, had no effect on call set-up within the 1-second "normal" time frame. OpenScape SBC completely rejected all these attacks. No vulnerabilities in OpenScape SBC were detected and all call features during the attack attempts remained fully operational.

6.7 RTP Protocol-Mutation Attack

Description

The Real-time Transmission Protocol (RTP) is used to deliver real-time audio (i.e., VoIP) and video content over IP networks. It is the primary protocol for delivery of voice conversations in SIP-based systems. OpenScape SBC is SIP-based, but in the test bed all voice content was carried in a secure form of RTP, Secure RTP or SRTP, where the content is encrypted.

Also, the OpenScape SBC nodes do not typically handle media streams directly. These typically pass, in encrypted SRTP form, between calling parties in the OpenScape architecture. Due to this it was expected that OpenScape SBC nodes would drop RTP and SRTP messages.

The Mutated-RTP attack, generated by Spirent Studio Security, was sent at high volume triggering rate limiting and at below-the-rate-limit rates under 300 pps for OpenScape SBC.

Observations and Analysis - PASS

No faults were reported, and we confirmed that the Mutated-RTP attack, launched against every IP address of each OpenScape SBC node individually, had no effect on call set-up within the 1-second normal time frame. OpenScape SBC completely rejected all these attacks. No vulnerabilities in OpenScape SBC were detected and all call features during the attack attempts remained fully operational.

6.8 UDP Protocol-Mutation Attack

Description

The User Datagram Protocol (UDP) is so-named because it is not a state-based protocol; a UDP datagram is sent and there is no additional follow-up, or state-based interactive messaging, to confirm it was received. Even so, UDP datagram messages, especially mutated UDP messages, can wreak havoc in a system that is not hardened to such attacks.

The Mutated-UDP attack, generated from the Spirent Studio Security, was sent at high volume triggering rate limiting and at below-rate-limit rates under 300 pps for OpenScape SBC.

The test was set up to attack OpenScape SBC interfaces using permutations of the many different and mutated UDP messages. The OpenScape node should completely block the attack.

Observations and Analysis - PASS

No faults were reported, and we confirmed that the Mutated-UDP attack, launched against every IP address of each OpenScape SBC node individually, had no effect on call set-up within the 1-second normal time frame. OpenScape SBC completely rejected all these attacks. No vulnerabilities in OpenScape SBC were detected and all call features during the attack attempts remained fully operational.

7 - Denial of Service Attacks

Various DoS attacks were directed at the OpenScape SBC system. The goal: to determine the continued availability and security of service in the face of attacks that apply elevated traffic to the same device interfaces that are handling high levels of production traffic. Often a targeted system will crash and need to be rebooted from an effective DoS attack.

The attacks were applied to OpenScape SBC interfaces individually, one at a time. During each attack, calls were placed between HQ-LAN and Remote-WAN phones, the connect times were clocked, and random features were exercised.

High-level open-source test scripts, as well as Spirent Studio Security were used to generate a dozen different DoS attacks. These collectively employed fixed and randomized source ports IP and MAC addresses, TTLs (time-to-live counters), TCP sequence numbers, payload, user-defined TCP header values, randomized protocol types and other values for the attack. Attack patterns included different load rates packets per second and duration of attacks.

The OpenScape SBC system was preconfigured and hardened to counter DoS attacks. The defenses included a Layer 3 integrated packet filter and a traffic-rate limiter. All of the DoS attacks exceeded the 300-pps rate limit that was configured in the OpenScape SBC nodes to counter DoS attacks. However, the attack loads were not high enough to deny sufficient bandwidth to regular production traffic, although that is exactly what some DoS attacks attempt to do. Subsequently, as long as rate limiting worked as expected, no DoS attacks should have had an effect.

A partial list of the DoS attacks launched as part of this security assessment follows.

7.1 IPv4 and ICMP DoS

These were two discrete attacks: The IPv4 DoS attack, containing many IP message types, all directed at the OpenScape SBC port, was generated by the Spirent Studio Security. The ICMP (Ping) DoS attack was generated using a command-line software tool, HPING3. The ICMP attack delivered up to 10,000 pings per second, to the particular IP interface.

Observations and Analysis - PASS

No faults were reported, and we confirmed that the IPv4 and ICMP DoS attacks, launched against every IP address of each OpenScape SBC node individually, had no effect on call set-up time. OpenScape SBC completely rejected all these attacks. No vulnerabilities in OpenScape SBC were detected and all call features during the attack attempts remained fully operational. Rate limiting worked effectively in deflecting these attacks.

7.2 TCP and TCP Syn-Flood DoS

These were two discrete attacks. Both were generated by the Spirent Studio Security. These attacks consisted of over 100,000 protocol-message variations, mutations and fragmentations of both legitimate and invalid TCP messages.

First, a TCP DoS attack many variations, mutations and fragmentations of both legitimate and invalid TCP messages were launched at 630 packets per second. This was followed by a second

TCP DoS attack, consisting largely of a flood of TCP SYN messages, delivered at 730 packets per second.

Observations and Analysis – PASS *

Aberrant responses were received from two of the three OpenScape SBC interfaces in most cases, in response to the TCP-based DoS attacks:

- Aberrant responses were received from two of the SBC IP interfaces – the 10.10.88.17 interface, this was the local IP address of the failover SBC, not the primary, and the 10.10.88.18 interface, which was the Virtual IP (VIP) address for both SBCs.
- We did not experience any aberrant behavior or responses from the primary SBC IP=10.10.88.15.
- The aberrant behavior did not occur all the time. It occurred in response to either of the TCP attacks about 65-70% of the time, with either of the two sensitive IP interfaces.
- It seemed that running the previous DoS, an ICMP host-unreachable flood, first would tend to prompt the aberrant behavior, but we are uncertain of a direct case-and-effect relationship, since the aberrant responses did not occur all the time.
- The aberrant responses from the target IP interfaces of the SBC were many TCP ACK and RST reset.
- Our procedure was to place a phone call as we launched a new DoS attacks. In the case of the first TCP DoS, we are fairly confident that the first call completion was appreciably delayed – on the order of 15 seconds (from last digit dialed to first ring). After this single delayed call, however, we observed no other subsequent effect on call completion. All calls subsequent to the first one completed within the one-second time frame, so the DoS attacks did not affect voice-call performance.
- Since the TCP DoS attacks both exceeded the 300-pps rate-limit, it seems that there may have been an issue with the SBC's imposition of rate-limiting.

*Upon further analysis and the inability to reproduce the anomaly, we did not see a reoccurrence of this problem. With a system reset, Unify has been able to mitigate the TCP-based DoS attack concerns.

7.3 UDP and UDP DNS-flood DoS

These were two discrete attacks, although both were generated by the Spirent Studio Security. These attacks consisted of over 100,000 protocol-message variations, mutations and fragmentations of both legitimate and invalid UDP messages.

Observations and Analysis - PASS

No faults were reported, and we confirmed that the attacks had no effect on call set-up time. OpenScape SBC completely rejected all these attacks. No vulnerabilities were detected and all call features during the attack attempts remained fully operational. Rate limiting worked effectively in deflecting these attacks.

7.4 ICMP and ICMP port-unreachable DoS

These were two discrete attacks, although both were generated by the Spirent Studio Security. These attacks consisted of over 100,000 protocol-message variations, mutations and fragmentations of both legitimate and invalid ICMP messages.

Observations and Analysis - PASS

No faults were reported, and we confirmed that the ICMP and ICMP port-unreachable DoS attacks, launched against every IP address of each OpenScape SBC node individually, had no effect on call set-up time. OpenScape SBC completely rejected all these attacks. No vulnerabilities in OpenScape SBC were detected and all call features during the attack attempts remained fully operational. Rate limiting worked effectively in deflecting these attacks.

7.5 ARP DoS

The ARP DoS, generated by the Spirent Studio Security, consisted of over 100,000 protocol-message variations, mutations and fragmentations of both legitimate and invalid ARP messages.

Observations and Analysis - PASS

No faults were reported, and we confirmed that the ARP DoS attack, launched against every IP address of each OpenScape SBC node individually, had no effect on call set-up time. OpenScape SBC completely rejected all these attacks. No vulnerabilities in OpenScape SBC were detected and all call features during the attack attempts remained fully operational. Rate limiting worked effectively in deflecting these attacks.

8 - Other Attacks and Security Tests

The following is a summary of compound exploits and other tests and analyses conducted as part of the OpenScape SBC V9 security assessment:

8.1 Published Vulnerability Attacks

Two attacks, both produced by the Spirent Studio Security, were launched against all interfaces on the OpenScape SBC nodes incorporating software vulnerabilities from the latest list of published software vulnerabilities. The first attack was more general in nature, delivering thousands of attempted exploits applicable to many platforms and operating systems. The second attack focused on 630 published critical software vulnerabilities.

Observations and Analysis - PASS

No faults were reported, and we confirmed that the two Published Vulnerability attacks had no effect on call set-up time. OpenScape SBC completely rejected these attacks. No vulnerabilities in OpenScape SBC were detected and all call features during the attack attempts remained fully operational.

8.2 Deregistering SIP Users/Devices

Deregistering legitimate SIP users is a method users by hackers to steal service by pirating eavesdropping a SIP registration and using it to register the IP of the hacker.

Observations and Analysis - PASS

We were unable to succeed at deregistering phones and capturing and re-using the registration information for an illicit user.

8.3 Brute Force Username/Password Attack

Various attempts, using several test scripts and the Hydra program, sought to gain access to OpenScape SBC nodes by using usernames and passwords from published lists of common usernames and passwords.

Observations and Analysis - PASS

We concluded that SSH and Web GUI access to management are not susceptible to brute force username and password attack in the current configuration. SSH authentication was limited to key-based authentication, so the service rejected any attempts to log in via a username and password combination.

Tests failed to determine the specific version of SSH service and no specific vulnerability was found. We observed that only the administered IP address, embedded in the white-list file, has access to the management interface. OpenScape SBC's IDS/IPS was successful at temporarily blocking connection attempts regardless of whether the traffic rate from the same source exceeded or was under the threshold of 300 packets per second.

8.4 Protocol Fuzzing Attack

Ixia's BreakingPoint system was used to produce a SIP protocol fuzzing attack. This is where malformed or semi-malformed SIP messages, which exploit different aspects of the SIP grammar, are injected to overwhelm, confuse or crash the system's call control.

Observations and Analysis - PASS

The SIP protocol-fuzzing attacks were ineffective and successfully thwarted by OpenScape SBC. Rate limiting may have been responsible for this success. During the attacks we were still able to establish legitimate calls within a 1-second normal time frame and call features we tested worked without problems.

8.5 Heartbleed SSL Exploit

The heartbleed exploit, identified last year within the OpenSSL (libopenSSL) heartbeat implementation, can permit an attacker to obtain private keys from a vulnerable target host. This was checked in a 2014 security audit and OpenScape SBC was found to be invulnerable to the heartbleed exploit. OpenScape SBC was rechecked during this audit to assure V9 was still immune.

Observations and Analysis - PASS

Numerous heartbleed checks were performed by Nessus against the OpenScape SBC running HTTPS. No heartbleed vulnerability was found. Nessus confirmed that there was no heartbleed vulnerability in OpenScape SBC V9.

8.6 Ghost Attack

In January 2015 NIST announced a network-exploitable attack, called Ghost, which allows a remote hacker to penetrate a system and, using two specific commands, gain access and run arbitrary code. Here is the advisory from SUSE: web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0235

Observations and Analysis - PASS

A check of the Ghost vulnerability in the OpenScape SBC was conducted and there is no vulnerability in the OpenScape SBC system.

8.7 Venom Attack

A SUSE security vulnerability, exploiting floppy disk controller commands to crash or take over a server, called VENOM, was identified in May 2015. For the advisory from SUSE see: https://www.suse.com/security/cve/CVE-2015-3456.html

We applied a check to see if the vulnerability existed in OpenScape SBC.

Observations and Analysis - PASS

No vulnerability to the Venom exploit exists, our check found. The OpenScape products are not vulnerable to this attack.

8.8 Shellshock (Bash bug) Attack

In the fall of 2014 a Web-server vulnerability, affecting most Linux versions, was announced. It is called "shellshock," also known as the "bash bug," and as "GNU Bash CVE-2014-6271 Remote Code Execution Vulnerability." Using this vulnerability a remote attacker can execute arbitrary code or produce a denial-of-service condition.

Observations and Analysis - PASS

The OpenScape SBC system was checked using Nikto, and again using Sparta, and no vulnerability to shellshock/bash was found.

9 - About Miercom

Miercom has published hundreds of network product analyses in leading trade periodicals and other publications. Miercom's reputation as the leading, independent product test center is undisputed.

Private test services available from Miercom include competitive product analyses, as well as individual product evaluations. Miercom features comprehensive certification and test programs including: Certified Interoperable™, Certified Reliable™, Certified Secure™ and Certified Green™. Products may also be evaluated under the Performance Verified™ program, the industry's most thorough and trusted assessment for product usability and performance.

10 - Use of This Report

Every effort was made to ensure the accuracy of the data contained in this report but errors and/or oversights can occur. The information documented in this report may also rely on various test tools, the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the vendors that were reasonably verified by Miercom but beyond our control to verify to 100 percent certainty.

This document is provided "as is," by Miercom and gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained in this report.