Security Assessment Report
DR120521

Siemens Enterprise Communications
OPENSCAPE VOICE V7

October 2012

Miercom

www.miercom.com

Table of Contents

1.0 Executive Summary

OpenScape Voice V7, a stand-alone software-based IP PBX, was evaluated for its inherent security resilience, without the use of external countermeasures such as UTM gateways or firewalls. Miercom used threats that included basic DoS attacks up through protocol mutations such as ICMP, IPv4and Sip attacks to try to disable the system.

Siemens built-in internal security was able to preserve normal operations while blocking attempted exploits and provided maximum uptime for users, confirming the IP-PBX is an effective High Availability System. The performance of the OpenScape Voice and ability to protect call processing functions when subjected to malicious exploits and attacks was impressive. Siemens OpenScape Voice V7 is recognized as Miercom Certified Secure.

The purpose of the test was to determine if there were any relevant security vulnerabilities that could be leveraged to the detriment of a customer using OpenScape Voice. We compared the resiliency of OpenScape Voice to that of other IP PBX and Unified Communications solutions on the market. Overall, the OpenScape products proved more secure than the majority of other products tested to date.

All tests conducted on OpenScape products were inside the internal network. No external security measures were used. We stressed the inherent resiliency of the hardened OpenScape systems themselves. Tests included a complex set of exploits distributed by security tools and scripts to challenge the capabilities of the OpenScape system. The OpenScape Voice proved resilient through multiple batteries of tests.

OpenScape Voice was tested without any additional security countermeasures employed other than what is provided inherently in the system. The internal countermeasures that are built into the firewall of OpenScape Voice were enabled during testing. The approach and methodology utilized in these tests are based on knowledge that Miercom, in collaboration with leading security experts, has collected from years of working in VoIP pre- and post-deployment site surveys and security assessments.

This document provides an overview of the more noteworthy exploit attempts that were conducted. In some test cases, specific details were intentionally omitted to avoid the use of this information to reverse-engineer exploits for VoIP products. The products tested were configured in accordance with guidance from Siemens Enterprise Communications, documented in their OpenScape Voice Security Checklist that in effect, enhances the resiliency of the systems.

Key Findings and Conclusions

- DoS attacks against OpenScape Voice were blocked by the internal firewall of the system
- OpenScape system blocked all other attempted exploits while preserving the system's normal operation
- OpenScape Voice SIP signaling interfaces blocked attempted ICMP, IPv4, and SIP attacks
- OpenScape Voice testing proved effective for High Availability providing maximum uptime for users

Test results are detailed in the following sections. We were impressed with the performance of the OpenScape systems with their ability to protect call processing functions when subjected to malicious exploits and attacks. Miercom is pleased to present the Certified Secure Award to OpenScape Voice V7.

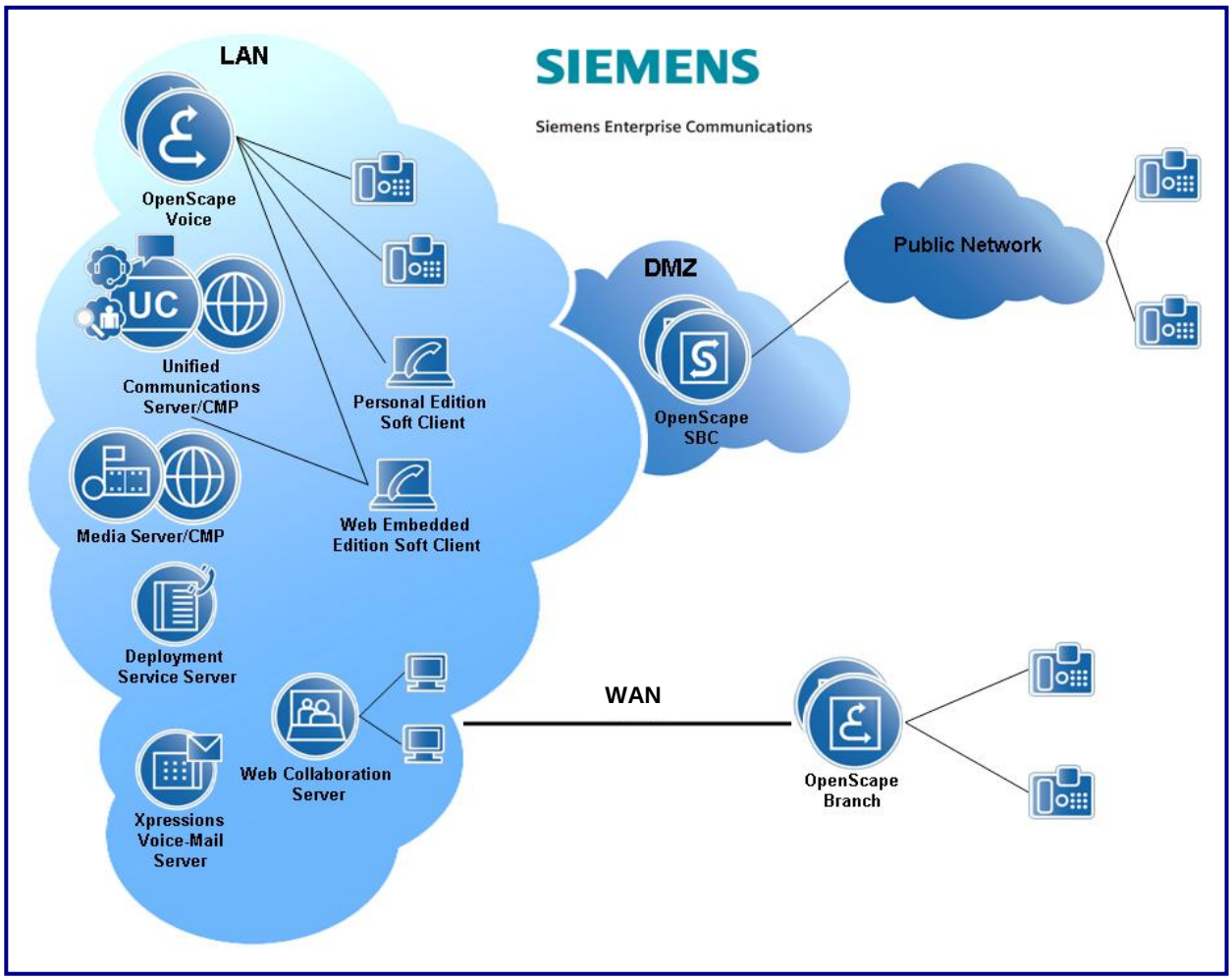
Rob Smithers
CEO
Miercom

2.0 OpenScape Voice Deployment Diagram

A representative diagram for an enterprise network for OpenScape Voice is depicted below. The OpenScape Voice system was connected in a “High Availability” configuration that would be more typical in a larger enterprise configuration. The High Availability configuration consists of contingency measures to maintain availability in case the OpenScape system application fails. Each OpenScape server has eight Ethernet ports, in two sets of four, enabling fully-redundant network connections. The testing included OpenStage 60/80 SIP phones for call uptime verification. Security assessment of OpenScape Voice V7 was made without use of any security gateways, firewalls or SBC in the deployed topology.

Exact configuration and tools used in testing for this project is proprietary for the protection of the security testing program and the vendor being tested.

Logical Configuration of OpenScape Voice V7



3.0 How We Did It

To conduct the tests reported in this report, we used a combination of test tools including customized proprietary test scripts, commercial vulnerability scanning tools and open-source security assessment products. A VoIP network infrastructure typical of a mid-sized enterprise to support OpenScape Voice was used as much as possible. The viability of each attack and the risk of compromise of OpenScape were evaluated and compensating measures were recommended to rectify or mitigate the suspect vulnerabilities. Additional details are shown in the OpenScape Voice Deployment Diagram.

The objective was to compromise the OpenScape Voice V7 system and prevent it from successfully delivering real-time voice communications. We also attempted to gain surreptitious access to the OpenScape system for the purposes of placing unauthorized calls, or compromising and intercepting presumed secure VoIP communications. The OpenScape systems were evaluated in a secured internal network. The tests were conducted without external security countermeasures employed to the OpenScape systems. The objective was to assess the resiliency of IP PBX components first and then subsequently assess the additional protection provided by the underlying network.

The OpenScape Voice network consisted of two OpenScape Voice nodes and OpenStage 60/80 SIP phones. The two OpenScape Voice nodes were implemented for High Availability in the event an outage occurred on one. High Availability testing included pulling the power supply, performing a soft shutdown and unplugging the Ethernet cables from one of the nodes to examine whether calls remained functional.

OpenScape Voice V7 was evaluated while installed in a standard quality assurance test environment. A perimeter assessment was done to identify paths through the network that could be used to assault the systems by a potential attacker. Several paths (i.e. SIP signaling, the administrative interface) were identified that merited exercising to look for flaws. These paths were then exercised as potential attack vectors that are further detailed within this report.

The security certification was conducted in three phases: research, reconnaissance and execution. Preparation began weeks prior to the actual testing date, with tools, attacks planned and pre-tested prior to the start of actual testing. Preparations included researching public sources, such as Google, Bug Traq, CVE, and security advisory, as well as Miercom internal research. The scanning and enumeration part involved learning the network topology, including services running, ports open/filtered, protocols, operating systems, program names and version numbers. The tools used for port-scanning and enumeration included Nmap and Netcat. Several rounds of analysis were performed on the data path that led from the phone to the OpenScape system to identify server-side issues. This involved rebooting the IP phones, making calls, and examining the internal state of the OpenScape servers using the operator console.

SIP torture tests were conducted against the Linux kernel TCP stack. The endpoints were tested for any potential information leakage that could be used against the phone or to attack the OpenScape Voice servers. Attempts to gain surreptitious access to the OpenScape systems were executed, along with attacks directed to the management interfaces (HTTPS, SSH).

Penetration test tools for running attacks/exploits, security scans including protocol interaction with mutated traffic, common vulnerability exploit tests, Denial of Service (DoS) and SIP server torture tests (RFC 4475) included proprietary test scripts and the open-source security assessment products, Offensive Security and Mu Dynamic's Mu Studio Security Service Analyzer. Mu Dynamic's (http://www.mudynamics.com) Mu Studio Security analyzer provides a complete service assurance solution for determining the reliability, availability and security of IP-based applications and services.

The Mu Studio Security Analyzer actively and methodically probes for vulnerabilities using attack vectors. These vulnerabilities may exist as the result of an insecure protocol implementation, a known security flaw or even a bug in the beta code of the product. The Mu Studio Security Analyzer was used to perform protocol mutations, published vulnerabilities and also external attacks using test cases and custom scripts. The Mu solution is highly automated with lights-out fault isolation. It can help speed the remediation of software flaws by providing actionable reports and complete data on any fault.

We used Nmap to scan each system in the OpenScape infrastructure to see what vulnerabilities were present. If Nmap finds vulnerabilities, it will generate a short report displaying each vulnerable port. Once the ports that were open were isolated, the types of attack were planned for bombarding the exposed system.

The Metasploit Project is an open-source computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. Its most well-known sub-project is the Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive, and security research.

The viability of each attack and the risk of compromise to the SUT were evaluated and compensating measures were recommended to rectify or mitigate the suspected vulnerabilities.

The tests in this report are intended to be reproducible for customers who wish to recreate them with the appropriate test and measurement equipment. Current or prospective customers interested in repeating these results may contact reviews@miercom.com for additional details on the configurations applied to the system under test and test tools used in this evaluation. Miercom recommends customers conduct their own needs analysis study and test specifically for the expected environment for product deployment before making a selection.

4.0 Metasploit Attacks

Description

The Metasploit Project, an open-source computer security project, provides information about security vulnerabilities, while helping with penetration testing and IDS signature development. Metasploit uses known exploits to identify any vulnerabilities or security holes that could be used as a gateway for hackers.

Configuration

This modularity of allowing the combination of any exploit with any payload is the major advantage of the Framework. It assists the tasks of attackers, exploit writers, and payload writers.

Purpose

Metasploit can be used to test the vulnerability of computer systems to protect them, and it can be used to break into remote systems.

Expected Results

It is expected that OpenScape will not be compromised on any level.

Observations

OpenScape Voice deflected or avoided 100% of penetration attempts on all attempted attack surfaces.

Analysis

PASS

We were unable to gather any information or detect any vulnerabilities that would help lead to a successful penetration of the server. The primary filtered ports were port 22 on the billing interface for both nodes of OpenScape Voice, and standard SIP ports 5060 and 5061. Penetration attempts were made on these ports to determine if a common exploit was not properly addressed. In our testing, no penetration attempts succeeded.

5.0 Nmap Scans

Nmap was used to scan each system in the OpenScape Voice V7 environment for open ports. A single IP address or an IP address range may be inputted into Nmap to reveal vulnerable devices on the network. A system with open ports can pose a threat if they are not securely implemented.

5.1 Nmap Scan against OpenScape Voice Admin Interface

Description

An Nmap scan was performed against the OpenScape Voice Administrator interface to find port vulnerabilities.

Observations

PASS

The Nmap report revealed that the OpenScape Voice billing interface had port 22 or SSH (Secure Shell) open. SSH is used for secure communication between two network devices. SSH is secure because it communicates over an encrypted channel. In this network, the SSH port on the Admin interface may be used for modifying or viewing configurations on the server from a remote location. It is highly unlikely that this open SSH port can be used as a valid entry point, nor is it susceptible to eavesdropping because the communication channel is highly encrypted and being an old, tested-by-time protocol, well protected.

5.2 Nmap Scan against SIP Signaling Interfaces

Description

An Nmap scan was performed against the OpenScape Voice SIP Signaling interface to find vulnerable ports.

Observations

PASS

The Nmap software could not identify any open ports during the scan. We conclude the SIP signaling interface on OpenScape Voice V7 is secure. Ports 5060 and 5061 are filtered appropriately.

6.0 Protocol Mutations and Vulnerability Scans

Protocol mutation attacks created by the Mu Studio Security Analyzer were directed at OpenScape Voice to test for vulnerabilities in protocol implementation. The mutation engine maps the attack surface (OpenScape Voice) looking for fault conditions. These include highly specific, stateful test cases that are built based on the state, structure and semantics of protocols, as well their interdependencies on other protocols.

The protocol mutation attacks described below included individual, unique deviation from the standard operation in a protocol implementation. Secure and robust targets should handle mutated packets by dropping them, but an insecure target with protocol implementation flaws would respond abnormally. The OpenScape Voice systems were analyzed for stateful and stateless mutation possibilities for a particular protocol and all protocols on which they depend.

The open SSH port on OpenScape Voice was not vulnerable. We captured packets that were going to and from the Administrator interface that was connected to a network PC with SSH using NMap and Wireshark. After reviewing the packet captures, we did not see any private information that would help us successfully penetrate or eavesdrop the encrypted communication channel.

The following sections are a partial list of protocol mutation attacks that were performed.

6.1 DHCP Mutation Attack

Description

DHCP is a computer format for transferring binary computer information in the form of a low level computer language from one computer or device to another to relay the proper information for determining the dynamic IP address. With dynamic IP addressing, each time a device connects with another or to a network, the IP address could change. The proper transfer of the IP address data is of paramount importance in keeping a device performing smoothly. Corruption of this data could cause a failure of the device.

Configuration

The test was configured to attack the OpenScape Voice interfaces using DHCP INFORM messages.

Purpose

To determine whether the dynamic IP address could be corrupted by the attack from the mutated DHCP protocol.

Expected Results

OpenScape Voice servers will completely block the attempted attacks due to their static IP configuration and continue their normal operation.

Observations

The DHCP mutation attack was run with 11,843 different INFORM message attacks. Each variant/attack vector carried a single protocol mutation directed towards the OpenScape Voice (OSV) Admin interface and SIP Signaling interfaces. Each test against OSV ran for 6 minutes and 35 seconds.

Analysis

PASS

All attack vectors were handled successfully and no faults were reported. OpenScape Voice dropped all mutated packets and did not send any error messages. No vulnerabilities in the DHCP protocol implementation at OpenScape Voice were detected. All calling features during the attack remained fully operational.

6.2 ICMPv4 Protocol Mutation Attacks

Description

This protocol mutation attack was generated by the Mu Studio Security Analyzer as a part of its suite of proprietary protocol mutation data. ICMP is a communications protocol for the proper format of digital messages and procedures for the exchange of messages between computing systems. Its main purpose is to work within the computer operating system of the network, monitoring the status of a requested service, host or router, and determining their availability. Another use of this protocol is to relay messages. It can also be used as a diagnostic ping or network tracer tool. IP addressing is crucial to its correct operation. Any corruption of the IP address could cause failure of the system.

Configuration

The test is configured to attack the OpenScape Voice interfaces using ICMPv4 echo requests and fragmented echo requests.

Purpose

The purpose of the ICMPv4 attacks is to determine whether the OpenScape Voice system will block the mutated packets and maintain full system functionality.

Expected Results

OpenScape Voice system will completely block the attempted attacks and continue their normal operation.

Observations

The ICMPv4 protocol mutation attack against the OpenScape Voice Admin interface contained 50,647 different variants/attack vectors. These variants were implemented in ICMP echo requests and ICMP fragmented echo request messages. When attempts were made to direct the attack against the Voice SIP Signaling interfaces, the attack failed because the OSV successfully discarded the ICMP requests.

Analysis

PASS

All attack vectors were handled successfully and no faults were reported. OpenScape Voice dropped all mutated packets and did not send any error messages. No vulnerabilities in the ICMPv4 protocol implementation on the OpenScape systems were detected. ICMPv4 attacks against the SIP Signaling interface were unable to run because it does not permit ICMPv4 requests.

During the ICMP attack against the Admin interface on OpenScape Voice, there was a noticeable pattern that would occur every few minutes. Each time the Mu analyzer sent ICMP requests, the attack script would report “connection-refused.” This was due to the firewall on the OpenScape system blocking the constant ICMP requests for a one minute period. After one minute, the attack script started again and was immediately blocked.

6.3 IPv4 Protocol Mutation Attacks

Description

IPv4 is the most widely used Internet communications protocol for the proper formatting of digital messages and procedures for the exchange of messages between computing systems. It is a connectionless protocol for use with the Ethernet family of networking technologies for local area networks. It functions on the “best effort delivery” philosophy, in that the network does not guarantee the delivery of the data or a quality of service level. The users of this protocol are not guaranteed a specific bit rate or delivery time. It is dependent on the current traffic load. The IPv4 protocol is limited in its IP addresses due to its 32-bit architecture. These IP addresses are vulnerable to attack and corruption. If this data were corrupted, it could lead to device failure. We tested to determine whether the dynamic IP address could be corrupted by the attack from the mutated IPv4 protocol.

Configuration

The test is configured to attack the OpenScape Voice interfaces using IPv4 datagrams and fragmented datagrams.

Purpose

The purpose of the IPv4 attack is to determine whether the OpenScape systems will appropriately block all malformed packets.

Expected Results

The OpenScape Voice systems will completely block the attempted attacks and continue their normal operation.

Observations

The IPv4 protocol mutation attack was run against the OpenScape Voice interfaces. The IPv4 attacks that were run against the Admin interface of OpenScape Voice contained 33,341 variants/attack vectors consisting of IPv4 datagrams and IPv4 fragmented datagrams. The SIP Signaling interfaces on OpenScape Voice rejected all attacks.

Analysis

PASS

All attack vectors were handled successfully and no faults were reported. The OpenScape Voice interfaces dropped all mutated packets and did not return any error messages. No vulnerabilities in the IPv4 protocol implementation at the OpenScape Voice were detected.

6.4 SIP Torture Test against OpenScape Voice

Description

This attack attempted to exploit product vulnerabilities in handling Session Initiation Protocol (SIP) traffic that had been deliberately modified to cause abnormal handling of the traffic.

This test case contained a valid, non-malformed message and then 99 malformed messages. The Target response to this test helped establish a baseline from which to analyze all other results from test cases in this suite:

- **Success.** When the target successfully responds to the valid test case, the target is handling valid messages appropriately. If other test cases in this suite find faults, the problem is most likely within this specific area of the protocol implementation.
- **Failure.** When the target does not respond successfully to the valid test case, the target is not handling valid messages appropriately. Other test cases in this suite are likely to find faults. The target might have larger problems in the overall protocol implementation, or you might need to edit the protocol options.

Other Background

All calls using the SIP protocol require a source and destination URI (phone number) which allow the server to establish communication between two endpoints. SIP communication can be established using TCP and UDP, and for more secure communications, Transport Layer Security (TLS). TCP and UDP commonly use port 5060, while TLS typically uses port 5061. SIP messages are made up of Register, Invite, Ack, Cancel, Bye and Options messages.

Configuration

The test was configured to attack the OpenScape Voice SIP Signaling interfaces using SIP Invite, Cancel, Options and Register messages using TLS. TLS was forced for all connections, and the TCP protocol was not allowed.

Purpose

The purpose of the test is to determine whether the OpenScape system will appropriately block all malformed packets.

Expected Results

It is expected that OpenScape Voice will completely block the attempted attacks and continue its normal operation. Malformed packets would be dropped. Valid formed SIP packets would be processed.

Observations

Since TLS was forced for all connections on OpenScape Voice, each attempted test was rejected by OpenScape Voice.

Analysis

PASS

Forced TLS on OpenScape Voice proved to be highly secure and prohibited the SIP attack from running. Phones remained fully operational, maintaining call functionality.

6.5 SIP Protocol Mutation Attacks against OpenScape Voice

Description

This attack attempted to exploit product vulnerabilities in handling Session Initiation Protocol (SIP) traffic that has been deliberately modified to cause abnormal handling of the traffic. All calls using the SIP protocol require a source and destination URI (phone number) that allows the server to establish communication between two entities. SIP communication can be established using TCP and UDP, or for more secure communications, by using Transport Layer Security (TLS). TCP and UDP commonly use port 5060, while TLS typically uses port 5061. SIP messages are made up of Register, Invite, Ack, Cancel, Bye and Options.

Configuration

The test was configured to attack OpenScape Voice using SIP Invite-Cancel messages.

To permit the test to run, the protocol specifically opened for communication transport was UDP over port 5060. Siemens engineers also provided authentication credentials. The digestmd5 username and password were configured to match the source URI. With the default configuration that forces TLS for all connections and without the valid credentials, all attempts to perform the test were rejected.

Purpose

The purpose of the test is to determine whether the OpenScape system will appropriately block all malformed SIP packets to and from unregistered users.

Expected Results

It is expected that the OpenScape Voice will completely block the attempted attacks and continue its normal operation.

Observations

The SIP Invite-Cancel messages directed towards OpenScape Voice ran for 25 hours. Attempts to speed up the execution of the test resulted in OpenScape Voice blacklisting the tester for registering too frequently. Two faults were reported. The first fault, with a confidence level of 1 out of 5 (low) reported that OpenScape Voice responded with a connection time-out to an “authorized.headers.repeated” mutation variant. The second fault, with a confidence level of 3 out of 5 (medium) was reported when OpenScape Voice responded with a connection time-out to an “ipv4.address.invalid” mutation variant. Captures of these faults have been provided to Siemens engineers for further investigation. No impact was observed to call processing when these faults were recorded.

Analysis

PASS

Two low level faults were reported due to an unexpected response by the server to the test variant. Operation of the system and call processing did not appear to be impacted. We do not consider these faults significant. If not for Siemens engineers opening up UDP transport and providing credentials specifically to allow this test to run, these faults would not otherwise have been reported by the Mu. In the standard system configuration that forces TLS for all connections, and without valid credentials, all attempts to perform the SIP test were rejected.

7.0 Other Analysis Conducted

The following is a summary of the compound exploits and other analysis conducted in the OpenScape Voice V7 Security Assessment:

Port Scanning and Enumeration – Open source tool, Nmap was used to scan the OpenScape servers for unused open ports, OS fingerprinting, version numbers, supported protocols, running services, and other information that could be used to attack the OpenScape servers. Only in-use ports were open, ICMP only, at the Admin and Billing interfaces of the OpenScape Voice server. All ports except those in use were filtered or closed. ICMP was disabled at the SIP signaling interface and the majority of port scans and enumeration attempts were successfully blocked.

Integer and Buffer Overflow Tests – These mutations add, insert or replace input with a large number of random bytes, in an effort to cause data to exceed the boundaries of its specified location. Overflow attacks exploit computer methods used to store integers, which are variables that represent real, non-fractional numbers. We represent integers in decimal format (using 10 numerals, 1-10), but computers store integers in binary format (using two numerals, 1 and 0). If the operation produces a value larger than the maximum integer size for the data, an integer overflow occurs. Miercom verified that these potential integer overflow conditions did not cause buffer overflows.

Fragmented Attacks – Fragmented packets were used to infiltrate and cause degradation in server performance. Such fragmented packets can get past Access Lists (ACLs) in stateless packet filtering deployment and be further used to cause DoS. Several types of attacks - teardrop, overlapping fragment and tiny fragment - were tested with the OpenScape server. No vulnerabilities were found after the fragmented attacks were applied.

Analysis

PASS

No abnormalities were detected in these directed attacks.

8.0 Denial of Service Attacks

Denial of Service (DoS) attacks were generated and directed at the OpenScape Voice SIP signaling interface and the administration interface to gain insights into reliability, availability and security of service in the face of DoS attacks or extreme amounts of service level traffic. While attacking the OpenScape servers, our objective was to saturate them to the extent that they could not respond to legitimate traffic, thereby becoming unresponsive and slow, or they would crash and reboot. Any of these conditions would lead to failures at the SIP phones.

Metasploit, Offensive Security and Mu Studio Security were used to configure 28 different DoS attacks with fixed and randomized source ports (IP and MAC addresses). TTLs, TCP sequence numbers, payload, user-defined TCP header values, randomized protocol types and other values for the attack packets were also configured. Attack patterns included different start/end rates (packets/sec), duration of attacks and number of attack iterations. Target availability and response time was verified at defined intervals during the attacks using ICMP.

The OpenScape Voice servers were preconfigured and hardened to counter DoS attacks. The defenses included a Layer 3 integrated packet filter and a traffic rate limiter. Incoming traffic was monitored using integrated IDS (Intrusion Detection System). The rate threshold configured to counter DoS attacks was set to 200 pps, so any IP address exceeding this dynamically was added to the blacklist. All subsequent messages from that IP were blocked for an administrator-defined time interval. In this case, the block period was 60 seconds.

A partial list of DoS attacks used and their results are discussed below:

8.1 ICMP Flood DoS

Description

These IP packets comprise an ICMP flood, which is a DoS attack that is also known as a ping flood or Smurf attack. During the attack, the Mu Analyzer sent large amounts of ICMP packets to the target system in an attempt to crash its TCP/IP stack and cause it to stop responding to TCP/IP requests.

Configuration

The DoS attack consisted of 100,000 packets per second and was directed at the OpenScape Voice and OpenScape Branch interfaces. The ability of OpenScape Voice to maintain existing calls and place new calls was monitored and any faults would be recorded.

Purpose

The purpose of the test is to verify the firewall effectiveness of OpenScape Voice when faced with large amounts of ICMP packets.

Expected Results

OpenScape Voice will detect and block the ping flood with no disruption in maintaining services.

Observations

The attacks were blocked and the server log indicated that the IP addresses (static and spoofed random addresses) of the attack platform were blacklisted for 60 seconds.

Analysis

PASS

No calls were dropped and the SIP phones did not lose service. The OpenScape systems are unharmed by the DoS attack and continue normal operation during and after the test.

8.2 IPv4 DoS Attacks

Description

The attack consisted of IP packets containing datagrams and fragmented datagrams, which is a DoS attack designed to flood the system. During the attack, the Mu Analyzer sent large amounts of IPv4 packets to the target system in an attempt to crash the TCP/IP stack and cause it to stop responding to TCP/IP requests.

Configuration

The DoS attack was set at 100,000 packets per second and was directed at the OpenScape Voice interfaces. The ability of OpenScape Voice to maintain existing calls and place new calls was monitored and any faults would be recorded.

Purpose

To verify the firewall effectiveness of OpenScape Voice when these systems are faced with large amounts of IP packets.

Expected Results

OpenScape Voice will detect and block the ping flood with no disruption in maintaining services.

Observations

The attacks were blocked and the server log indicated that the IP addresses (static and spoofed random addresses) of the attack platform were blacklisted for 60 seconds. No calls were dropped and the SIP phones did not lose service.

Analysis

PASS

No calls were dropped and the SIP phones did not lose service. The OpenScape systems are unharmed by the DoS attack and continue normal operation during and after the attack.

8.3 Attacks with Spoofed SIP Phone IP Address

Description

Attacks were repeated with the source IP address of the attack packets spoofed to be the IP address of the SIP phones. The IP address of the SIP phones could be obtained by using open source tools like ping sweeps, Nmap or from the SIP phone itself. The objective of this test was to blacklist the IP addresses of the SIP phones and thereby cause disruption in telephone service. These tests were only possible when user credentials were obtained from engineers of Siemens Enterprise Communications.

Test

The OpenScape Voice Server was configured for a rate limiting threshold of 200 packets/sec. DoS attacks with the spoofed source address of the SIP phone were directed at the OpenScape Server at a user-defined packet rate.

Observation

With the packet rate of the DoS attacks set at 100,000 packets/second, the spoofed IP address of the SIP phones was added to the blacklist for 60 seconds. Phones lost SIP signaling, and telephone service was disrupted for 60 seconds (as long as the IP address was blacklisted). After the blacklist period expired, the IP addresses of the phones were removed from the blacklist. The phone became available and telephone service resumed. Although this attack can render individual phones temporarily unavailable, the OpenScape Voice Server successfully thwarted this attack from causing a widespread outage.

Analysis

PASS

Although this attack can render individual phones temporarily unavailable, the OpenScape Voice server successfully thwarted this attack from causing a widespread or prolonged outage. The primary reason for phone disruption is due to the device, and not the servers themselves. No SIP transactions were improperly relayed, and the sole issue remains within the phone's NIC being flooded and not an actual vulnerability.

9.0 High Availability of OpenScape Voice Server

Description

The high availability of the OpenScape Voice application was demonstrated by deploying an OpenScape Voice cluster with two servers while implementing the use of a Virtual IP address (VIP). One OpenScape Voice server node was intentionally made to fail and telephone service was observed for any disruptions.

Configuration

High Availability testing included pulling the power supply, performing a soft shutdown and unplugging the Ethernet cables from one of the nodes to examine whether calls remained functional.

See the “How We Did It” section on page 5 for more information.

Purpose

To verify and assess carrier grade reliability and high availability of the OpenScape Voice (OSV) deployment.

Expected Results

It is expected that all calls will seamlessly remain connected during a failover of OSV Node A to OSV Node B.

Observations

Each server of the cluster is assigned a VIP. Upon failure of one server, the peer server took over the VIP of the failed server and assumed session control for all devices assigned to that VIP. Upon failure of OpenScape Voice Server A, VIP A was taken over by OpenScape Voice Server B.

Analysis

PASS

Existing SIP calls remained connected during the failure of Node A and new calls could also be placed. Once the OpenScape Voice Server A was brought back online, it once again resumed the role of an active server, and full redundant operation was restored with VIP A taken over by OpenScape Server A.

10.0 Verification of Cryptographic TLS

Description

This test confirmed that the TLS-protected connections used for SIP signaling are configured to use sound cryptographic operating values. The SUT is checked for the cryptographic algorithms used, key length and use of proper TLS protocol options. The likelihood of improperly configured TLS cryptographic parameters depended on the initial configuration at time of deployment, expertise of the installer(s), documentation, etc. If weak cryptographic algorithms and vulnerable or outdated TLS protocol options are used, it is possible the TLS protection mechanism can be compromised.

Test

The TLS cryptographic parameters were tested for use of strong keys and secure algorithms and the recommended TLS protocol settings.

Observations

Diagnostic tools were used to confirm that proper TLS configuration for OpenScape Voice V7 was employed.

Analysis

PASS

It was verified that 128-bit encryption was utilized for OpenScape Voice V7.