# Securing a Virtualized Session Boarder Controller – Huawei's vSBC

The Session Border Controller, which connects an organization's internal network with carrier services and the Internet, has emerged as a key juncture in VoIP networks. And that makes the SBC particularly attractive to, and susceptible to attacks from, malicious attackers.

Complicating SBC security is the trend towards virtualizing the SBC function – where the SBC consists of software that runs as one client process on a multi-client server host.

Huawei Technologies Co., Ltd. offers such a product, its Virtualized SBC, or vSBC a virtualized software version of Huawei's legacy SE2900 Session Border Controller appliance. Miercom's job: to determine the susceptibility of the vSBC to a malicious attacker – whether internal or external.

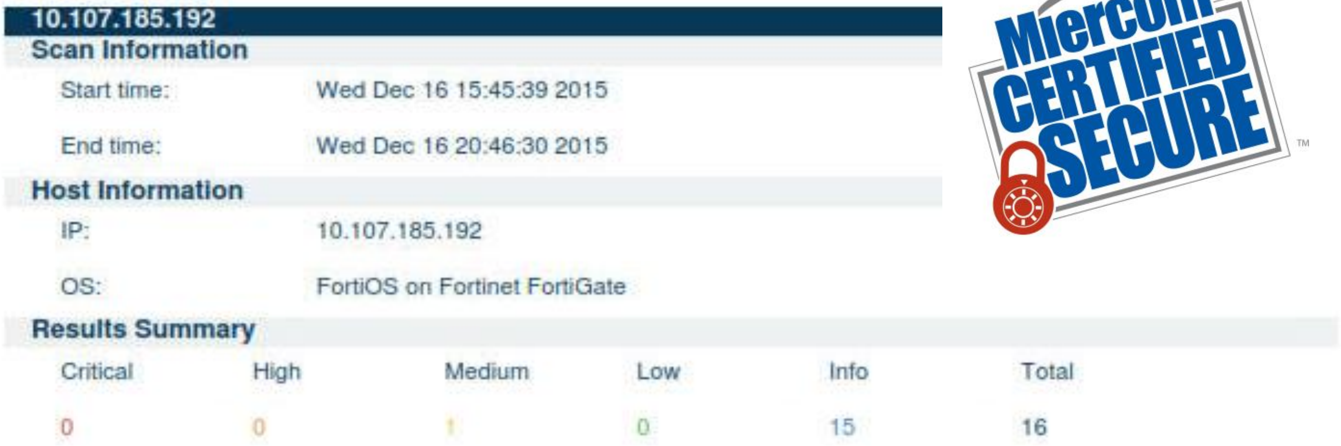
## What We Measured

The purpose of the testing was to uncover any evident security vulnerabilities that a assailant could exploit to disrupt the proper, normal operation of the vSBC.

Most exploits against the vSBC were launched from an inside source, on the same internal switched network, with no other security protection between the assailant and the hardened vSBC system. Tests included a broad and complex set of exploits launched by numerous security tools and scripts to stress and penetrate the vSBC system.

## Key Findings

- Huawei's vSBC blocked every DoS and DDoS attack launched against it.
- The vSBC package includes numerous effective features for protecting the system from access by unauthorized individuals. Password control is bulletproof.
- vSBC also proved resilient to hundreds of thousands of fuzzing attacks and protocol mutations launched against it. The system is impressively hardened.
- Various tests were conducted to see if popular exploits used for service theft and fraud would work. The system effectively blocked all of these.
- Scans of the system by leading penetration-scanning tools revealed no known vulnerabilities.



**10.107.185.192**

**Scan Information**

Start time: Wed Dec 16 15:45:39 2015

End time: Wed Dec 16 20:46:30 2015

**Host Information**

IP: 10.107.185.192

OS: FortiOS on Fortinet FortiGate

**Results Summary**

| Critical | High | Medium | Low | Info | Total |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 0 | 15 | 16 |

For 28 years Miercom has been the world leader in independent security and performance testing. Miercom has published hundreds of network-product-comparison analyses that are free to consumers. Testing is based on a methodology that is jointly co-developed with the vendor. We're Miercom, it's what we do.

Scan to read the full report or visit
www.miercom.com/Huawei