PBX: Private Branch Exploit!: A Measurement Study on Vulnerable PBXs

Avinash Rajaraman, Saurabh Singh Rana

Department of Computer and Informational Science, University of Florida

PBX (Private Branch Exchange)

- A PBX (private branch exchange) is a telephone system within an enterprise that switches calls between enterprise users on local lines while allowing all users to share a certain number of external phone lines.
- The main purpose of a PBX is to save the cost of requiring a line for each user to the telephone company's central office.

Why is a vulnerable PBX bad?

A vulnerable PBX could lead to an assortment of problems

- A successful compromise could mean that the attacker could gain a lot of money while racking up massive bills to both the owner of the PBX and the provider.
- More often a compromised PBX would allow the attacker to eavesdrop calls made by the company
- The attacker could also spoof calls from the company, thus defaming and damaging the company's reputation
- The impact is that Telecom companies lost over 7.46 billion dollars in 2015 alone!

Methodology

To find out exactly how many PBXs were present, we used "Shodan.io", which scans the entire ipv4 spectrum to discover devices. Shodan gave us a huge list containing nearly 53000 PBXs.

We concentrated on vendor of PBX namely Asterisk, as 35000 or 65% of the PBXs belonged to asterisk.

We then looked for the documented vulnerabilities of Asterisk PBX in the CVE Database, and compared to the Asterisk PBXs discovered by Shodan.

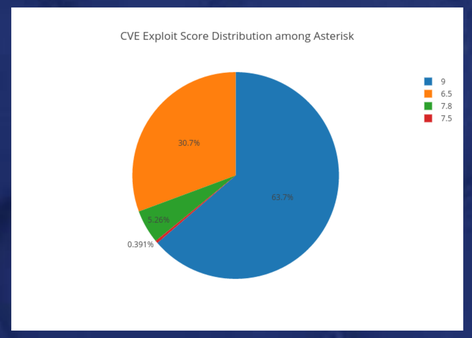
We only considered vulnerabilities of a CVE score of 6.5 or greater.

Takeaway: *One in 10 PBXs are vulnerable to Dos and Exec Code attacks*

Observations

We observed the following from the data given by Shodan:

- The total number of PBXs discoverable was 52,567 and The number of asterisk machines amongst them was 35,004.
- A total of 8834 vulnerabilities were found.
- 5880 PBXs were found to be vulnerable, having a CVE score greater than 6.5.



- The vulnerabilities were some forms of Denial of Service and Remote code execution.
- There were over 8000 asterisk PBXs on whom we could not comment on, due to the lack of data.

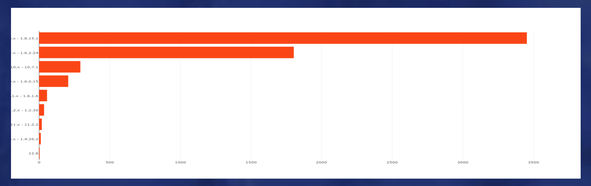
CONCLUSION

We found that despite extensive and comprehensive documentation, nearly one in ten PBXs were vulnerable. Nearly 3800 PBXs had a vulnerability of a CVE score 9 or greater. This is just a rough estimate of the vulnerable PBXs that are out there, with more data and with better device fingerprinting, it can only be concluded that more vulnerable PBXs will be found.

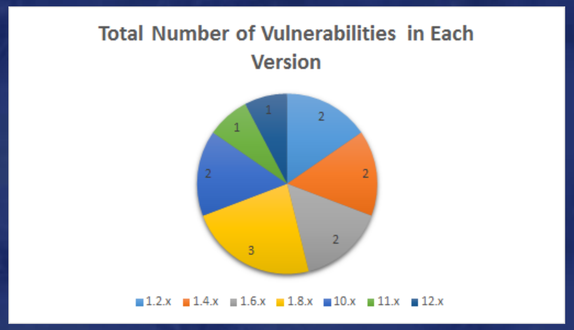
Results

We found the following results:

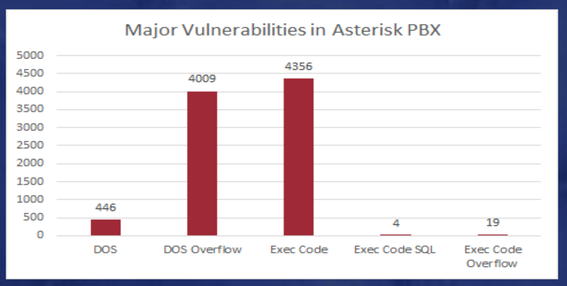
- The vulnerable PBX version that is being used the most are versions 1.8-1.8.15.1



- 1.8.x versions of Asterisk PBX has the most number of vulnerabilities.



- 4455 PBXs are vulnerable to Dos overflow attacks.
- 4379 PBXs are vulnerable to some form of a remote code execution attack.



- Around 3800 asterisk PBXs have a vulnerability of a 9 or greater in CVE rating scale.