- research
- .gitignore
- README.md
- bluekeep_dos.py
- bluekeep_poc.py
- requirements.txt

README

Bluekeep PoC

This repo contains research concerning CVE-2019-0708.

Bluekeep or CVE-2019-0708 is an RCE exploit that effects the following versions of Windows systems:

- Windows 2003
- Windows XP
- Windows Vista

About

Proof of concept for CVE-2019-0708

- Windows 7
- Windows Server 2008
- Windows Server 2008 R2

The vulnerability occurs during pre-authorization and has the potential to run arbitrary malicious code in the NT Authority\system user security context.

How it works

By sending a specially crafted packet an attacker is able to set the value for the Channel ID to something the RDP service isn't expecting, this causes a memory corruption bug that will create the conditions for Remote Code Execution to occur. Should the attacker choose to follow up with packets designed to take advantage of this flaw remote code execution can be achieved with System user privileges.

Setup

```
sudo apt install python python-dev python-setup
git clone https://github.com/ekultek/bluekeep
cd bluekeep
pip install -r requirements.txt
```

That should do what you need done and fix any issue you have.

Credits

Research by Ekultek and (VectorSEC)/NullArray

Development & Testing by Ekultek

Follow us on Twitter

- Ekultek
- VectorSEC

- **Python** 100.0%

In Closing

You can see some of our research, along with a list of potentially vulnerable targets under the research directory. We started with very little and decided that we weren't going to stop until we had a working exploit. I have been able to execute commands on Windows XP with this PoC personally.

Note

There are no payloads. This is just a PoC. *HOWEVER* it is easily ported to an exploit since you can easily add payloads to this.