What is VENOM Vulnerability? How can you protect yourself?

The VENOM vulnerability affects all major CPU vendors, including Intel, AMD, and ARM. VENOM allows malicious actors to read the contents of a computer's memory and potentially execute code remotely.

If you have a vulnerable CPU, your computer could be at risk, so it's important to know how to protect yourself against this exploit!

What is VENOM Vulnerability?

VENOM stands for Virtualized Environment Neglected Operations Manipulation, and like other vulnerabilities, it's been around for quite some time.

Its code in the Common Vulnerabilities and Exposure database is CVE-2015-3456, which means the vulnerability was publicly disclosed in 2015 by Jason Geffner, a CrowdStrike senior security researcher. This vulnerability, first introduced in 2004, affected virtual machine devices and interfaces from QEMU, KVM, Xen, and VirtualBox from that period until it was fixed following the issue.

The VENOM vulnerability arises due to a weakness in QEMU's virtual floppy driver, which allows network attackers to penetrate the virtualization fabric, including any machine in a given data network.

This vulnerability has a major impact on data security; this can cause problems with millions of virtual machines at risk of being exploited. It is usually enabled through various default configurations that grant different commands execution permissions.

If the network attackers successfully execute their operation, they can move horizontally from the attacked virtual machine and gain access to your network server. They can then access other virtual machines on the network. That will definitely put your data at high risk.

How does the VENOM vulnerability work?

Picture 1 of What is VENOM Vulnerability? How can you protect yourself?

VENOM is a very malicious vulnerability that exists inside the virtual machine's floppy drive, so cyber attackers can exploit this vulnerability and use it to steal data from the affected virtual machines.

That is to say, in order to successfully perform their intrusion, the attackers need to have access to the virtual machine. They will then need to have access to the virtual floppy driver - the I/O ports. They can do this by transferring specially crafted codes and commands from the guest virtual machine to the compromised floppy

driver. The affected floppy driver then gives permissions to the virtual machine, allowing the hacker to interact with the underlying network server.

The VENOM vulnerability is mainly used in large-scale targeted attacks, such as cyber warfare, corporate espionage, and other types of targeted attacks. They can also create buffer overflows inside the virtual machine's floppy drive, get out of the virtual machine, and infiltrate others inside the hypervisor, a process known as traversing.

Furthermore, attackers can gain access to bare metal platform hardware and view other structures in the hypervisor network. Hackers can migrate to other independent platforms and monitors on the same network. That way, they can access your organization's intellectual property and steal sensitive information, such as Personal Identifiable Information (PII).

They can even steal your Bitcoins if you have BTC tokens on the system. Once they get past the attack and gain unrestricted access to your server's local network, they can grant a competitor access to your server's network.

Which systems are affected by VENOM?

Picture 2 of What is VENOM Vulnerability? How can you protect yourself?

VENOM can be easily exploited by cybercriminals on many different systems. The systems most commonly attacked with the VENOM vulnerability include Xen, VirtualBox, QEMU, Linux, Mac OS X, Windows, Solaris, and any other operating system built on QEMU hypervisors or virtualization.

That's a problem for major cloud providers like Amazon, Citrix, Oracle, and Rackspace because they rely too heavily on QEMU-based virtual systems that are vulnerable to VENOM. However, you don't have to worry much because most of these platforms have developed strategies to protect virtual machines from cybercriminals' attacks.

For example, according to Amazon web services, there is no risk posed by the VENOM vulnerability regarding AWS customer data.

How to protect yourself from VENOM

If you're worried about your data being stolen due to the VENOM vulnerability, don't worry. There are ways to protect yourself from it.

One way you can protect yourself is to use patches. As cyberattacks through VENOM became particularly widespread, patches were developed by software vendors as a means of redressing vulnerabilities.

Xen and QEMU systems, the systems most affected by the VENOM vulnerability, have separate patches available to the public. Be aware that any QEMU patch that protects you from the VENOM vulnerability will require you to restart the virtual machine.

System administrators running KVM, Xen, or QEMU clients should install the latest patches released by their vendors. It is best to follow the vendor instructions and verify the application for the most recent VENOM patch.

Here are some vendors that have released patches for the VENOM vulnerability:

1. QEMU.
2. Red Hat.
3. Xen Project.
4. Rackspace.
5. Citrix.
6. Linode.
7. FireEye.
8. Ubuntu.
9. Suse.
10. Debian.
11. DigitalOcean.
12. f5.

Another option to protect yourself from the obvious VENOM vulnerability is to use systems that are not vulnerable to this type of attack, such as Microsoft Hyper-V, VMWare, Microsoft Linode, and Amazon AWS. These systems are safe from VENOM-based vulnerabilities, as they are not vulnerable to attacks from cybercriminals using that particular vulnerability.