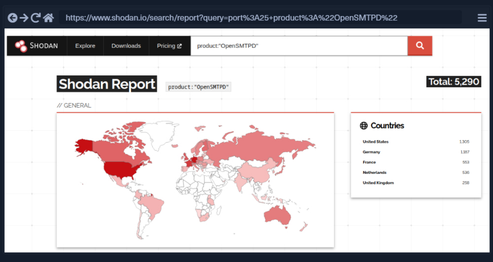
Latest Email Service Vulnerabilities

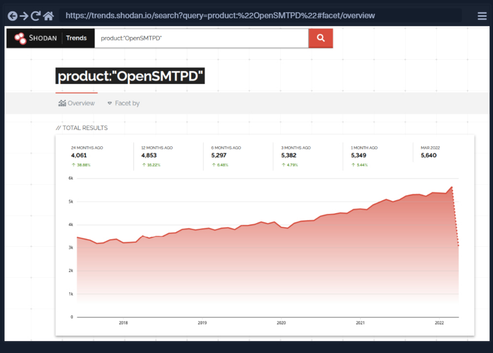
One of the most recent publicly disclosed and dangerous Simple Mail Transfer Protocol (SMTP) vulnerabilities was discovered in OpenSMTPD up to version 6.6.2 service was in 2020. This vulnerability was assigned CVE-2020-7247 and leads to RCE. It has been exploitable since 2018. This service has been used in many different Linux distributions, such as Debian, Fedora, FreeBSD, and others. The dangerous thing about this vulnerability is the possibility of executing system commands remotely on the system and that exploiting this vulnerability does not require authentication.

According to Shodan.io, at the time of writing (April 2022), there are over 5,000 publicly accessible OpenSMTPD servers worldwide, and the trend is growing. However, this does not mean that this vulnerability affects every service. Instead, we want to show you how significant the impact of an RCE would be in case this vulnerability were discovered now. However, of course, this applies to all other services as well.

Shodan Search



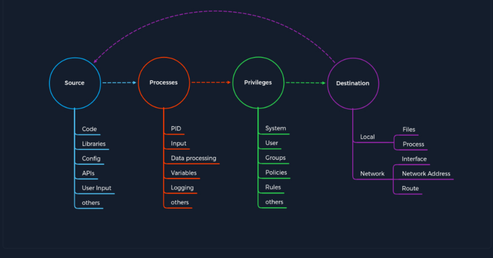
Shodan Trend



The Concept of the Attack

As we already know, with the SMTP service, we can compose emails and send them to desired people. The vulnerability in this service lies in the program's code, namely in the function that records the sender's email address. This offers the possibility of escaping the function using a semicolon (`;`) and making the system execute arbitrary shell commands. However, there is a limit of 64 characters, which can be inserted as a command. The technical details of this vulnerability can be found here.

The Concept of Attacks



Here we need to initialize a connection with the SMTP service first. This can be automated by a script or entered manually. After the connection is established, an email must be composed in which we define the sender, the recipient, and the actual message for the recipient. The desired system command is inserted in the sender field connected to the sender address with a semicolon (`;`). As soon as we finish writing, the data entered is processed by the OpenSMTPD process.

Initiation of the Attack

Step	Remote Code Execution	Concept of Attacks - Category
1.	The source is the user input that can be entered manually or automated during direct interaction with the service.	`Source`
2.	The service will take the email with the required information.	`Process`
3.	Listening to the standardized ports of a system requires `root` privileges on the system, and if these ports are used, the service runs accordingly with elevated privileges.	`Privileges`
4.	As the destination, the entered information is forwarded to another local process.	`Destination`

This is when the cycle starts all over again, but this time to gain remote access to the target system.

Trigger Remote Code Execution

Step	Remote Code Execution	Concept of Attacks - Category
5.	This time, the source is the entire input, especially from the sender area, which contains our system command.	`Source`
6.	The process reads all the information, and the semicolon (`;`) interrupts the reading due to special rules in the source code that leads to the execution of the entered system command.	`Process`
7.	Since the service is already running with elevated privileges, other processes of OpenSMTPD will be executed with the same privileges. With these, the system command we entered will also be executed.	`Privileges`
8.	The destination for the system command can be, for example, the network back to our host through which we get access to the system.	`Destination`

An exploit has been published on the Exploit-DB platform for this vulnerability which can be used for more detailed analysis and the functionality of the trigger for the execution of system commands.

Next Steps

As we've seen, email attacks can lead to sensitive data disclosure through direct access to a user's inbox or by combining a misconfiguration with a convincing phishing email. There are other ways to attack email services that can be very effective as well. A few Hack The Box boxes demonstrate email attacks, such as Rabbit, which deals with brute-forcing Outlook Web Access (OWA) and then sending a document with a malicious macro to phish a user, SneakyMailer which has elements of phishing and enumerating a user's inbox using Netcat and an IMAP client, and Reel which dealt with brute-forcing SMTP users and phishing with a malicious RTF file.

It's worth playing these boxes, or at least watching the Ippsec video or reading a walkthrough to see examples of these attacks in action. This goes for any attack demonstrated in this module (or others). The site ippsec.rocks can be used to search for common terms and will show which HTB boxes these appear in, which will reveal a wealth of targets to practice against.

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left