Google shares the source code of Tsunami, an enterprise vulnerability scanning tool

From now on, Tsunami will no longer be a Google product but will instead be maintained by the open source community.

Recently, Google decided to release the source code of the Tsunami enterprise network vulnerability scanning tool on GitHub. According to **Google Tsunami** can be extended to detect serious vulnerabilities with the lowest error rate.

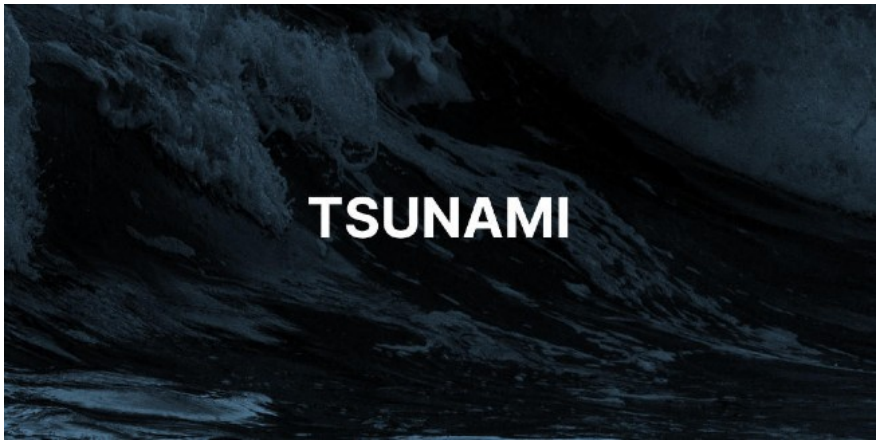
Tsunami was previously used internally within Google. However, from now on, everyone can access this tool via free source code on GitHub. Tsunami can scan large-scale enterprise networks, including millions or thousands of internet-connected systems.

After posting on GitHub, Tsunami will no longer be an official Google product. Instead, it is maintained, developed by the open source community. Google used to do the same thing with Kubernetes, a tool that helps automate deployment, replication, and management of container applications.

How does Tsunami work?

There are currently hundreds of system scanning tools available in the open source or commercialized form. But Tsunami is different from all that it can be used for large-scale businesses.

According to Google, Tsunami can be used for companies with network systems including hundreds of thousands of servers, workstations, networking equipment and IoT devices connected to the internet. Tsunami can also adapt to these very large, diverse networks, without the need to use different scanning tools for each device type.



The advantage of Tsunami is that it can scan large businesses as well

Google achieves this by dividing Tsunami into two main components and then adding the expandable plugin mechanisms at the top.

The first component is the scanner or scout module. It is responsible for scanning the system to detect ports that are not closed. It then examines each port and identifies the protocols and services running on each port to avoid flagging the port and device containing the vulnerability.

The second component is more complicated. It works based on the result of the first component. It will access each device and the port in contact with the device then select a list of vulnerabilities to test. Next, benign attacks and exploits will be deployed to see if the device is vulnerable.

Finally, with the plugin, Tsunami can expand its functionality in the future. Security researchers can add Tsunami new scanning methods for newly discovered vulnerabilities .

The current Tsunami version has plugins with the ability to test:

1. **Important UIs have been exploited:** Applications such as Jenkins, Jupyter and Hadoop Yarn have UIs that allow users to schedule or execute commands on the system. Therefore, if exploited, hackers can take advantage of the application's own functions to execute commands to attack the system.
2. **Poor security credentials:** Tsunami uses other open source tools like ncrack to detect weak passwords used by protocols and tools like SSH, FTP, RPD and MySQL.

Google said that in the coming months, they will equip Tsunami with new plugins to detect various ways of exploiting vulnerabilities. All plugins will be released via a separate repository on GitHub.

Minimize errors

Google said in the future Tsunami will focus on meeting the goals of high-end business customers that are the same size as themselves or businesses with large-scale, diverse networks of devices.

Tsunami's accuracy is the main goal Google pursues. The search giant hopes that with the contribution of the open source community, the level of error of this tool will be reduced to the lowest level possible.

You can download Tsunami here.

1.