Reputation Alerts

Suspicious Redirects

What is it?

A suspicious redirect is a redirect that has changed. Redirects are tracked with each scan, and if the redirect chain changes e.g. to a malicious website, or doesn't match the expected pattern a warning for suspicious behavior is thrown.

Where is it detected?

- Website Security Monitor

Alert Levels

- YELLOW: redirects may not be triggered on any visit, they might also be set on purpose by the web administrator.

Recommended Action

Check if the redirect is leading to the correct target. If the target is known as malicious, remove the redirect if possible immediately.

DNS Takeover

What is it?

A potential DNS takeover vulnerability was found. This means that an attacker may take control of a DNS server for resolving your hostname. The attacker can change the DNS record(s) to a server that he/she owns.
This issue type results from a misconfigured server. Domain's DNS records are controlled by DNS servers that anyone can use, but no one within this service claims the domain.

To perform a takeover, the name server has to be one of the currently known vulnerable DNS services that can be found here:

https://github.com/indianajson/can-i-take-over-dns?ref=blog.projectdiscovery.io

Where is it detected?

- Website Security Monitor

Alert Levels

- YELLOW: A potential DNS takeover vulnerability was found in the DNS configuration of your scanned website.

Recommended Action

- Delete the authoritative nameserver assigned to the domain
- (Re-)Activate the unused website (nameserver entry)

For more information, please check the following article:

https://blog.projectdiscovery.io/guide-to-dns-takeovers/

Revision #3
Created 11 August 2021 11:53:29 by Christian Baumgartner
Updated 9 January 2024 12:31:26 by Patrick Wall