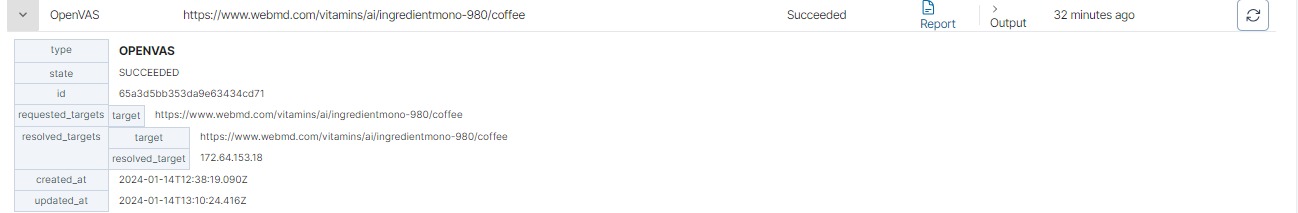
**NETWORK VULNERABILITY ASSESSMENT**

**Vulnerability Scan**

Vulnerability scans were conducted on selected servers, networks, websites, and applications.

This report contains the discovered potential risks from these scans. Risks have been classified into categories according to the level of threat and degree of potential harm they may pose.

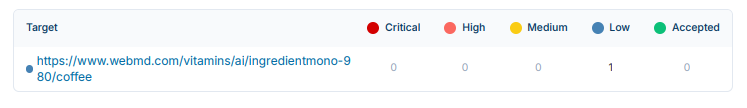
**Risks Detected**





This is the total number of risks found. High risks are the most severe and should be evaluated first. An accepted risk is one which has been manually reviewed and classified as acceptable to not fix at this time, such as a false positive or an intentional part of the system's architecture.

**Target Summary**



**Network Vulnerabilities**

The OpenVAS network vulnerability scan tests servers and internet connected devices for over 50,000 vulnerabilities. OpenVAS uses the Common Vulnerability Scoring System (CVSS) to quantify the severity of findings. 0.0 is the lowest severity and 10.0 is the highest.

**Description of Risk**

The remote host implements TCP timestamps and therefore allows to compute the uptime. The remote host implements TCP timestamps, as defined by RFC1323/RFC7323. A side effect of this feature is that the uptime of the remote host can sometimes be compute.

**Solution**

To disable TCP timestamps on linux add the line 'net.ipv4.tcp\_timestamps.