VULNERABILITY REPORT

This is a highly concise vulnerability report generated by Python-based modules, offering a comprehensive analysis of the target's security.

I. Overview

This report presents the results of a vulnerability assessment conducted on **20.7.1.11** using Python modules. The objective of this assessment is to provide a brief overview of the security posture of the target and identify potential vulnerabilities that could be exploited by attackers.

The main objective of the assessment was to identify vulnerabilities that could be used by attackers to compromise the confidentiality, integrity, or availability of the target. Python modules are used to automate the scanning process and identify potential vulnerabilities in the target.

Date: 2024-05-03 07:59

Target : 20.7.1.11

Type: vulnerability scanner

II. DNS Request

Check your domain name or the API website (https://networkcalc.com/api/)

III. Data about HTTP/HTTPS certificate

Metadata

protocol: https:
hostname: 20.7.1.11
port: 443

Certificate

protocol: https:
hostname: 20.7.1.11
port: 443
issued_to: TRAEFIK DEFAULT CERT
issued_by: TRAEFIK DEFAULT CERT
valid_from: 2024-05-03T07:45:26.000Z
valid_to: 2025-05-03T07:45:26.000Z
alternate_names:
['DNS:fbb5db66b52364c7f0e810ebcf2ef2f2.ee0cbdf4e78df89eb86ef0b78aadba3d.traef
serial_number: A349087060BA8601575797CCBE817EB4
fingerprint: E0:1D:8C:10:E8:EC:8E:90:6B:89:8C:2E:60:10:C1:12:52:4F:BC:
21
raw:
-----BEGIN CERTIFICATE-----
MIIDXjCCAkagAwIBAgIRAKNJCHBguoYBV1eXzL6BfrQwDQYJKoZIhvcNAQELBQAw
HzEdMBsGA1UEAxMUVFJBRUZJSyBERUZBVUxUIENFUlQwHhcNMjQwNTAzMDc0NT
WhcNMjUwNTAzMDc0NTI2WjAfMR0wGwYDVQQDExRUUkFFRklLIERFRkFVTFQgQ0V
VDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAKR/
WPR2n28jhdkJAl0O
6rgWb7Sz4er8u+Wde691lXq2B4v2y8gEbpLroA19oNzqjA0CNBOQtqyk2RSS+lXR
GeWiM1P1uKgTz2foRSt3G/H7iT/
x6yvq8ZbdLl495LsoyHktNzyTInCP6OvJPMCh
gyr0Ov6sgNz9lZKi5hpPfxOR71FvAQZellOin4kbqfH+XVzfKAkm6oIaSFH8tqmk
UpiirpUDdAW3JoM8fpaFt6I2j+oUNwJ8LAcQ9UAxn+YQrh9n7Nd34Xg/
vrjxhEGQ 5DAAHh+uakA4RILdZlswlPdL3jXyig+vQQ+x0jB/
sKvlr7167pW8WGotDVPxekWD
1lsCAwEAAaOBlDCBkTAOBgNVHQ8BAf8EBAMCA7gwEwYDVR0lBAwwCgYIKwYBBQU
AwEwDAYDVR0TAQH/
BAIwADBcBgNVHREEVTBTglFmYmI1ZGI2NmI1MjM2NGM3ZjBl

ODEwZWJjZjJlZjJmMi5lZTBjYmRmNGU3OGRmODllYjg2ZWYwYjc4YWFkYmEzZC50
cmFlZmlrLmRlZmF1bHQwDQYJKoZIhvcNAQELBQADggEBADeXjtJXOTaCPkPf3pqT
m8TFvxlZ9TqKdn8a37L1oHPIBbSHqJ1iXps/
aU4Ly03QnPD+Hmd61d90dVENMcXA ktXB2pQa0kppDN4QuCc4/
KUB36Fhop6HxxR4IJMTF/xwJQ7y3+2opkaK3OZweCeP WHqZp/
EDkWVxcZvznGSPKhnJ+cOsut4bI+0ffhLWaC4/VPRDURU+JucDpchUxDcv
2TtBXA8X49HCihu5zecjmW8egs+a9NqveXkkT+3xQAEP246HjNjBupzUwWD5tQn8
m2ksXjN+rcSS02S+5ORmazSZS85A2heXsaYOs8G1NOhyWktU/roJroa/
lz9CAgwi 3F8= -----END CERTIFICATE-----

IV. NMAP scan

[['20.7.1.11', 80, 'http', ''], ['20.7.1.11', 443, 'http', '']]

V. Nikto scan

The server doesn't support compression.

Target URL don't use any redirection

Target URL isn't protected by a basic HTTP authentication

The anti-clickjacking X-Frame-Options header is not present.

The X-XSS-Protection header is not defined.

VI. Potential vulnerabilities

CVE associated with http

Service: http, Version:

- CVE-2023-44487
- CVE-2013-4407
- CVE-2007-6423
- CVE-2018-19790
- CVE-2021-3007
- CVE-2016-4423
- CVE-2023-34062
- CVE-2023-45288
- CVE-2024-2653
- CVE-2015-2308
- CVE-2021-31618
- CVE-2007-6420

VI. Exploit find

VII. Recommendations

Keep your systems up-to-date with the latest security patches and updates for all software and services running on your domain or IP address. Vulnerabilities are often discovered and patched by vendors, so it's important to stay current with updates to minimize risk.

We also recommend reviewing the list of links provided in this report, which point to known exploits and vulnerabilities affecting various services. These links can provide additional information and guidance on how to mitigate these specific security risks for your domain or IP address.

By following these recommendations and staying vigilant against emerging security threats, you can help protect your systems and data from unauthorized access and exploitation.