VULNERABILITY REPORT

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

Summary

- **I. Overview**..... 1
- **II. DNS Request**.....1
- **III. Data about HTTP/HTTPS certificate**.....1
- **IV. NMAP scan**..... 2
- **V. Nikto scan**.....3
- **VI. Potential vulnerabilities**.....3
- **VII. Recommendations**.....4

I. Overview

This report presents the results of a vulnerability assessment conducted on **184.26.239.200** 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 03:56

Target : 184.26.239.200

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: 184.26.239.200
port: 443

Certificate

protocol: https:
hostname: 184.26.239.200
port: 443
issued_to: www.nissan.co.jp
issued_by: DigiCert TLS RSA SHA256 2020 CA1
valid_from: 2024-03-18T00:00:00.000Z
valid_to: 2025-03-19T23:59:59.000Z
alternate_names: ['DNS:www.nissan.co.jp', 'DNS:*.autech-elco.co.jp', 'DNS:*.carlifecollection.jp', 'DNS:*.dennoban.jp', 'DNS:*.e-sharemobi.com', 'DNS:*.nismo.co.jp', 'DNS:*.nissan-bs.co.jp', 'DNS:*.nissan-dealer.jp', 'DNS:*.nissan-fs.co.jp', 'DNS:*.nissan-global.com', 'DNS:*.nissan-kohki.jp', 'DNS:*.nissan-request.jp', 'DNS:*.nissan-shatai.co.jp', 'DNS:*.nissan.biz', 'DNS:*.nissan.co.jp', 'DNS:*.nissankyushu.co.jp', 'DNS:*.nissanmotor.jobs', 'DNS:*.ryukyu-nissan.co.jp', 'DNS:*.securedc.nissan.co.jp', 'DNS:*.tokyo-nissan.co.jp', 'DNS:e-sharemobi.com', 'DNS:nissan-global.com', 'DNS:nissan-heritage-collection.com', 'DNS:nissan-request.jp', 'DNS:nissan.co.jp', 'DNS:nissankyushu.co.jp', 'DNS:nissanmotor.jobs', 'DNS:securedc.nissan.co.jp']
serial_number: 03D928D0580FFFE1240EFF283C256F87
fingerprint: D2:2D:3F:18:2B:9F:C0:77:51:EF:1E:6F:D9:F8:3D:E6:2A:8D:2D:76
raw:
-----BEGIN CERTIFICATE----- MIIIFzCCBv+gAwIBAgIQA9ko0FgP/+EkDv8oPCVvhzANBgkqhkiG9w0BAQsFADBP
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMSkwJwYDVQQD
aWdpQ2VydCBUTFMgUlNBIFNIQTI1NiAyMDIwIENBMTAeFw0yNDAzMTgwMDAwMD
Fw0yNTAzMTkyMzU5NTlaMHIxCzAJBgNVBAYTAkpQMREwDwYDVQQIEwhLYW5hZ2F
YTEVMBMGA1UEBxMMWW9rb2hhbWEtU2hpMR4wHAYDVQQKExVOSVNTQU4gTU9U
Q08uLExURC4xGTAXBgNVBAMTEHd3dy5uaXNzYW4uY28uanAwWTATBgcqhkjOPQIB

BggqhkjOPQMBBwNCAAT5/6U0vctExqcGQXIXiWZn9C7r6VzZtR2zOF6alO4UIXE3
5PuAOXgKdxynNXfUxn23exZ33BUCdjLC8iWEg+jfo4IFlTCCBZEwHwYDVR0jBBgw
FoAUt2ui6qiqhIx56rTaD5iyxZV2ufQwHQYDVR0OBBYEFIeY4y3W55qJlEcZkcAn
OdDzKA/
iMIICOwYDVR0RBIICMjCCAi6CEHd3dy5uaXNzYW4uY28uanCCEyouYXV0
ZWNoLWVsY28uY28uanCCFiouY2FybGlmZWNvbGxlY3Rpb24uanCCDSouZGVubm9i
YW4uanCCESouZS1zaGFyZW1vYmkuY29tgg0qLm5pc21vLmNvLmpwghEqLm5pc3Nh
bi1icy5jby5qcIISKi5uaXNzYW4tZGVhbGVyLmpwghEqLm5pc3Nhbi1mcy5jby5q
cIITKi5uaXNzYW4tZ2xvYmFsLmNvbYIRKi5uaXNzYW4ta29oa2kuanCCEyoubmlz
c2FuLXJlcXVlc3QuanCCFSoubmlzc2FuLXNoYXRhaS5jby5qcIIMKi5uaXNzYW4u
Yml6gg4qLm5pc3Nhbi5jby5qcIIUKi5uaXNzYW5reXVzaHUuY28uanCCEioubmlz
c2FubW90b3Iuam9ic4IVKi5yeXVreXUtbmlzc2FuLmNvLmpwghcqLnNlY3VyZWRj
Lm5pc3Nhbi5jby5qcIIUKi50b2t5by1uaXNzYW4uY28uanCCD2Utc2hhcmVtb2Jp
LmNvbYIRbmlzc2FuLWdsb2JhbC5jb22CHm5pc3Nhbi1oZXJpdGFnZS1jb2xsZWN0
aW9uLmNvbYIRbmlzc2FuLXJlcXVlc3QuanCCDG5pc3Nhbi5jby5qcIISbmlzc2Fu
a3l1c2h1LmNvLmpwghBuaXNzYW5tb3Rvci5qb2JzghVzZWN1cmVkYy5uaXNzYW4u
Y28uanAwPgYDVR0gBDcwNTAzBgZngQwBAgIwKTAnBggrBgEFBQcCARYbaHR0cDov
L3d3dy5kaWdpY2VydC5jb20vQ1BTMA4GA1UdDwEB/
wQEAwIDiDAdBgNVHSUEFjAU
BggrBgEFBQcDAQYIKwYBBQUHAwIwgY8GA1UdHwSBhzCBhDBAoD6gPIY6aHR0cDov
L2NybDMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0VExTUlNBU0hBMjU2MjAyMENBMS00
LmNybDBAoD6gPIY6aHR0cDovL2NybDQuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0VExT
UlNBU0hBMjU2MjAyMENBMS00LmNybDB/
BggrBgEFBQcBAQRzMHEwJAYIKwYBBQUH
MAGGGGh0dHA6Ly9vY3NwLmRpZ2ljZXJ0LmNvbTBJBggrBgEFBQcwAoY9aHR0cDov
L2NhY2VydHMuZGlnaWNlcnQuY29tL0RpZ2lDZXJ0VExTUlNBU0hBMjU2MjAyMENB
MS0xLmNydDAMBgNVHRMBAf8EAjAAMIIBfgYKKwYBBAHWeQIEAgSCAW4EggFqAW
dwBOdaMnXJoQwzhbbNTfP1LrHfDgjhuNacCx+mSxYpo53wAAAY5PWjz0AAAEAwBI
MEYCIQDT1AmRFxtZri8lgxXToWquZsurwi98RtyX3Rf50S/
31wIhAINQ4mT3WV6b
sqeAifxEnwOV3pSGMCoNEDuFsC27Yo25AHUAfVkeEuF4KnscYWd8Xv340IdcFKBO
lZ65Ay/
ZDowuebgAAAGOT1o8tAAABAMARjBEAiAIz5O5qMvuum5DiOmUF3xnuZFK
2hGWbAR8VrIE1rm/SAIgFwi17yWWIXEzQLePgq2NygmJ9e0cCHAwHHPms/
8VqzgA
dgDm0jFjQHeMwRBBBtdxuc7B0kD2loSG+7qHMh39HjeOUAAAAY5PWjzTAAAEAwBH
MEUCICYCGqz3y/
MbOIiywZxefgxcZp88bEw6lCzAimy24AVdAiEAnHsNDLaTny2m saFgg/
g+OgrG4ADch676wVtNely+i6EwDQYJKoZIhvcNAQELBQADggEBALyLR9Fu
NjTi2o8bisg309qCPT/djgY2rj/vetkAnhd1q5Cz2zE89AH2pg1r+U4n4+eAJNVe
tlk1Q7+ZQD1pMkyX7Z0ayn4AQNN/
qKgrf6TVPFKiL8NsbZtBb92aakpb8xjgvKQi
ZVh83SA1Hw+SgR2gJHifZuQ+L0ivONFC71Tkcht7GZ94c6Rdv/QFDma/
gvHYtuqy
QmGiAGMMj+U6hq3+VUq5xeU2l7ofdxpUcwmr0QDxIoMSg6gD28jL+ILPw5MgyuaQ
bOtAO8lgi29GJdwxHmKpKisyVOihAfFO3qnyQ5QJ80AqMpgMGzObeWgovFJTpPV5
ia8HEl4vpun9N2c= -----END CERTIFICATE-----

IV. NMAP scan

[['184.26.239.200', 80, 'http', ''], ['184.26.239.200', 443, 'http', '']]

V. Nikto scan

Web server : AkamaiGHost

The server doesn't support compression.

Version of software might be found in the following header Mime-Version : 1.0

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.

The X-Content-Type-Options header is not set.

VI. Potential vulnerabilities

Service: http, Version:

+----------------------------+ | CVE associated with http | +============================+ | CVE-2015-2308 | +----------------------------+ | CVE-2023-44487 | +----------------------------+ | CVE-2023-34062 | +----------------------------+ | CVE-2016-4423 | +----------------------------+ | CVE-2023-45288 | +----------------------------+ | CVE-2021-31618 | +----------------------------+ | CVE-2007-6423 | +----------------------------+ | CVE-2021-3007 | +----------------------------+ | CVE-2007-6420 | +----------------------------+ | CVE-2013-4407 | +----------------------------+ | CVE-2024-2653 | +----------------------------+ | CVE-2018-19790 | +----------------------------+

Service: http, Version:

+----------------------------+ | CVE associated with http | +============================+ | CVE-2015-2308 | +----------------------------+ | CVE-2023-44487 | +----------------------------+ | CVE-2023-34062 | +----------------------------+ | CVE-2016-4423 | +----------------------------+ | CVE-2023-45288 | +----------------------------+ | CVE-2021-31618 | +----------------------------+ | CVE-2007-6423 | +----------------------------+ | CVE-2021-3007 | +----------------------------+ | CVE-2007-6420 | +----------------------------+ | CVE-2013-4407 |

+----------------------------+ | CVE-2024-2653 | +----------------------------+ | CVE-2018-19790 | +----------------------------+

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.