Scan Vulnerabilities Report

IMPLEX.NET

September 27 2021

PREPARED BY:
SecurityMetrics
1275 W. 1600 N.
Orem, UT 84057
USA

securityMETRICS®

Executive Summary

Scan target: **global.qwikcast.tv**
Scan ID: **10167830**
Scan Compliance Status: **Failing**
Maximum Score: **5.0**
Scan Expiration: **2021-12-27**
TCP/IP Fingerprint PS Estimate: **SonicWall Secure Mobile Access**
Start: **2021-09-27 13:02:13**
Finish: **2021-09-27 14:05:19**
Scan Length: **1:03:06**

Introduction

The target **fails** because at least one failing vulnerability was found.

Port Scan

Attackers use a port scan to find out what programs are running on your system. Most programs have known security weaknesses, so it is best practice to disable any unnecessary programs listed below.

Protocol	Port	Program
TCP	8172	Microsoft IIS httpd 10.0
TCP	7654	unknown
TCP	4024	tnp1-port
TCP	4022	dnox
TCP	1221	Microsoft HTTPAPI httpd 2.0
TCP	454	Microsoft IIS httpd
TCP	443	Microsoft IIS httpd 10.0
TCP	80	Microsoft IIS httpd 10.0

Scan Results

The following section lists all security vulnerabilities detected on your system. Vulnerabilities which cause you to fail PCI compliance have a score of 4.0 or higher and are listed in red.

Security Vulnerabilities

Protocol	Port	Service	Score	Summary

TCP	1221	www	5.0	**Title:** .bash_history Files Disclosed via Web Server **Synopsis:** The remote web server hosts what may be a publicly accessible .bash_history file. **Impact:** SecurityMetrics has detected that the remote web server hosts publicly available files whose contents may be indicative of a typical bash history. Such files may contain sensitive information that should not be disclosed to the public. **Resolution:** Make sure that such files do not contain any confidential or otherwise sensitive information, and that the files are only accessible to those with valid credentials. **Data Received:** The following .bash_history files are available on the remote server : - /.bash_history Note, this file is being flagged because you have set your scan to 'Paranoid'. The contents of the detected file has not been inspected to see if it contains any of the common Linux commands one might expect to see in a typical .bash_history file. - /cgi-bin/.bash_history Note, this file is being flagged because you have set your scan to 'Paranoid'. The contents of the detected file has not been inspected to see if it contains any of the common Linux commands one might expect to see in a typical .bash_history file. - /scripts/.bash_history Note, this file is being flagged because you have set your scan to 'Paranoid'. The contents of the detected file has not been inspected to see if it contains any of the common Linux commands one might expect to see in a typical .bash_history file. - /public/Content/themes/base/.bash_history Note, this file is being flagged because you have set your scan to 'Paranoid'. The contents of the detected file has not been inspected to see if it contains any of the common Linux commands one might expect to see in a typical .bash_history file. - /Account/.bash_history Note, this file is being flagged because you have set your scan to 'Paranoid'. The contents of the detected file has not been inspected to see if it contains any of the common Linux commands one might expect to see in a typical .bash_history file. - /Account/Login/.bash_history Note, this file is being flagged because you have set your scan to 'Paranoid'. The contents of the detected file has not been inspected to see if it contains any of the common Linux commands one might expect to see in a typical .bash_history file. - /public/Content/.bash_history Note, this file is being flagged because you have set your scan to 'Paranoid'. The contents of the detected file has not been inspected to see if it contains any of the common Linux commands one might expect to see in a typical .bash_history file.

TCP	443	www	✗ 5.0	**Title:** .bash_history Files Disclosed via Web Server **Synopsis:** The remote web server hosts what may be a publicly accessible .bash_history file. **Impact:** SecurityMetrics has detected that the remote web server hosts publicly available files whose contents may be indicative of a typical bash history. Such files may contain sensitive information that should not be disclosed to the public. **Resolution:** Make sure that such files do not contain any confidential or otherwise sensitive information, and that the files are only accessible to those with valid credentials. **Data Received:** The following .bash_history files are available on the remote server : -/Account/Login/.bash_history Note, this file is being flagged because you have set your scan to 'Paranoid'. The contents of the detected file has not been inspected to see if it contains any of the common Linux commands one might expect to see in a typical .bash_history file.
TCP	8172	www	√ 3.9	**Title:** SSL Certificate with Wrong Hostname **Synopsis:** The SSL certificate for this service is for a different host. **Impact:** The 'commonName' (CN) attribute of the SSL certificate presented for this service is for a different machine. **Resolution:** Purchase or generate a proper SSL certificate for this service. **Data Received:** The identities known by SecurityMetrics are : waws-prod-ch1-033.api.azurewebsites.windows.net global.qwikcast.tv The Common Name in the certificate is : waws-prod-ch1-033.publish.azurewebsites.windows.net The Subject Alternate Names in the certificate are : waws-prod-ch1-033.ftp.azurewebsites.windows.net waws-prod-ch1-033.publish.azurewebsites.windows.net

TCP	8172	www	√ 3.9	**Title:** Web Server HTTP Header Information Disclosure **Synopsis:** The remote web server discloses information via HTTP headers. **Impact:** The HTTP headers sent by the remote web server disclose information that can aid an attacker, such as the server version and languages used by the web server. **Resolution:** Modify the HTTP headers of the web server to not disclose detailed information about the underlying web server. **Data Received:** Server type : Microsoft IIS Server version : 10.0 Source : Microsoft-IIS/10.0
TCP	443	www	√ 3.9	**Title:** Web Server HTTP Header Information Disclosure **Synopsis:** The remote web server discloses information via HTTP headers. **Impact:** The HTTP headers sent by the remote web server disclose information that can aid an attacker, such as the server version and languages used by the web server. **Resolution:** Modify the HTTP headers of the web server to not disclose detailed information about the underlying web server. **Data Received:** Server type : Microsoft IIS Server version : 10.0 Source : Microsoft-IIS/10.0

TCP	443	www	√ 1.0	**Title:** CGI Generic Injectable Parameter **Synopsis:** Some CGIs are candidate for extended injection tests. **Impact:** SecurityMetrics was able to to inject innocuous strings into CGI parameters and read them back in the HTTP response. The affected parameters are candidates for extended injection tests like cross-site scripting attacks. This is not a weakness per se, the main purpose of this test is to speed up other scripts. The results may be useful for a human pen-tester. **Resolution:** n/a **Data Received:** Using the POST HTTP method, SecurityMetrics found that : + The following resources may be vulnerable to injectable parameter : + The 'UserName' parameter of the /Account/_ForgotPasswordTokenPage CGI : /Account/_ForgotPasswordTokenPage [UserName=%00whqhdu] -------- output -------- Enter Password Token <form action="/Account/_ForgotPasswordToken" id="fpFrm" method="po [...] <input id="UserName" name="UserName" type="hidden" value=".wh qhdu" /> <fieldset> <legend>Password Token Form</legend> ---------- /Account/_ForgotPasswordTokenPage [EmailAddress=&UserName=%00whqhdu&__RequestVerificationToken=I9xVGMFg9Om_-qKVLzMygSGtJJL4Z9ad81eJbImtBVTn5F1PqPVQoxrjGS2SkEw7XoWVZhVNLq8azRj2OziSoKxISB41] -------- output -------- Enter Password Token <form action="/Account/_ForgotPasswordToken" id="fpFrm" method="po [...] <input id="UserName" name="UserName" type="hidden" value=".wh qhdu" /> <fieldset> <legend>Password Token Form</legend> ----------
TCP	8172	www	√ 1.0	**Title:** TLS Version 1.2 Protocol Detection **Synopsis:** The remote service encrypts traffic using a version of TLS. **Impact:** The remote service accepts connections encrypted using TLS 1.2. See also : https://tools.ietf.org/html/rfc5246 **Resolution:** N/A **Data Received:** TLSv1.2 is enabled and the server supports at least one cipher.

TCP	454	www	√ 1.0	**Title:** TLS ALPN Supported Protocol Enumeration **Synopsis:** The remote host supports the TLS ALPN extension. **Impact:** The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports. See also : https://tools.ietf.org/html/rfc7301 **Resolution:** n/a **Data Received:** http/1.1
TCP	443	www	√ 1.0	**Title:** Missing or Permissive Content-Security-Policy frame-ancestors HTTP Response Header **Synopsis:** The remote web server does not take steps to mitigate a class of web application vulnerabilities. **Impact:** The remote web server in some responses sets a permissive Content-Security-Policy (CSP) frame-ancestors response header or does not set one at all. The CSP frame-ancestors header has been proposed by the W3C Web Application Security Working Group as a way to mitigate cross-site scripting and clickjacking attacks. See also : http://www.nessus.org/u?55aa8f57 http://www.nessus.org/u?07cc2a06 https://content-security-policy.com/ https://www.w3.org/TR/CSP2/ **Resolution:** Set a non-permissive Content-Security-Policy frame-ancestors header for all requested resources. **Data Received:** The following pages do not set a Content-Security-Policy frame-ancestors response header or set a permissive policy: - https://global.qwikcast.tv/ - https://global.qwikcast.tv/Account/Login - https://global.qwikcast.tv/Account/Login/loginLink - https://global.qwikcast.tv/Account/_ForgotPassword - https://global.qwikcast.tv/help - https://global.qwikcast.tv/home

TCP	454	www	√ 1.0	**Title:** SSL Cipher Suites Supported **Synopsis:** The remote service encrypts communications using SSL. **Impact:** This plugin detects which SSL ciphers are supported by the remote service for encrypting communications. See also : https://www.openssl.org/docs/man1.1.0/apps/ciphers.html http://www.nessus.org/u?3a040ada **Resolution:** n/a **Data Received:** Here is the list of SSL ciphers supported by the remote server : Each group is reported per SSL Version. SSL Version : TLSv12 High Strength Ciphers (>= 112-bit key) Name Code KEX Auth Encryption MAC ---------- ---------- --- ---- ---------- --- RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256 RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384 ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1 ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1 AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1 AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1 ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256 ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384 RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256 RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256 The fields above are : {Tenable ciphername} {Cipher ID code} Kex={key exchange} Auth={authentication} Encrypt={symmetric encryption method} MAC={message authentication code} {export flag}
TCP	443	www	√ 1.0	**Title:** Web Application Potentially Sensitive CGI Parameter Detection **Synopsis:** An application was found that may use CGI parameters to control sensitive information. **Impact:** According to their names, some CGI parameters may control sensitive data (e.g., ID, privileges, commands, prices, credit card data, etc.). In the course of using an application, these variables may disclose sensitive data or be prone to tampering that could result in privilege escalation. These parameters should be examined to determine what type of data is controlled and if it poses a security risk. ** This plugin only reports information that may be useful for auditors ** or pen-testers, not a real flaw. **Resolution:** Ensure sensitive data is not disclosed by CGI parameters. In addition, do not use CGI parameters to control access to resources or privileges. **Data Received:** Potentially sensitive parameters for CGI /Account/Login : Password : Possibly a clear or hashed password, vulnerable to dictionary attack Potentially sensitive parameters for CGI /Account/Login/loginLink : Password : Possibly a clear or hashed password, vulnerable to dictionary attack

TCP	1221	www	√ 1.0	**Title:** Web Application Sitemap **Synopsis:** The remote web server hosts linkable content that can be crawled by SecurityMetrics. **Impact:** The remote web server contains linkable content that can be used to gather information about a target. See also : http://www.nessus.org/u?5496c8d9 **Resolution:** n/a **Data Received:** The following sitemap was created from crawling linkable content on the target host : - http://global.qwikcast.tv:1221/ Attached is a copy of the sitemap file.
TCP	1221	www	√ 1.0	**Title:** Web Application Cookies Not Marked Secure **Synopsis:** HTTP session cookies might be transmitted in cleartext. **Impact:** The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies. Note that this plugin detects all general cookies missing the 'secure' cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag. See also : https://www.owasp.org/index.php/SecureFlag **Resolution:** Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision. If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data. **Data Received:** The following cookie does not set the secure cookie flag : Name : __RequestVerificationToken Path : / Value : Gu2uT40rfAnxS8Gj-1Eo8leHGTRSxjMboPMJV69sRIFQNFLeS0ETiunNgumUdpabJkwbx9ZP0otMlvhjB9M59x9nFMg1 Domain : Version : 1 Expires : Comment : Secure : 0 Httponly : 1 Port :

TCP	8172	www	√ 1.0	**Title:** TLS ALPN Supported Protocol Enumeration **Synopsis:** The remote host supports the TLS ALPN extension. **Impact:** The remote host supports the TLS ALPN extension. This plugin enumerates the protocols the extension supports. See also : https://tools.ietf.org/html/rfc7301 **Resolution:** n/a **Data Received:** http/1.1
TCP	454	www	√ 1.0	**Title:** TLS Version 1.2 Protocol Detection **Synopsis:** The remote service encrypts traffic using a version of TLS. **Impact:** The remote service accepts connections encrypted using TLS 1.2. See also : https://tools.ietf.org/html/rfc5246 **Resolution:** N/A **Data Received:** TLSv1.2 is enabled and the server supports at least one cipher.
TCP	443	www	√ 1.0	**Title:** SSL Root Certification Authority Certificate Information **Synopsis:** A root Certification Authority certificate was found at the top of the certificate chain. **Impact:** The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain. See also : https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10) **Resolution:** Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies. **Data Received:** The following root Certification Authority certificate was found : |-Subject : C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority |-Issuer : C=US/O=The Go Daddy Group, Inc./OU=Go Daddy Class 2 Certification Authority |-Valid From : Jun 29 17:06:20 2004 GMT |-Valid To : Jun 29 17:06:20 2034 GMT |-Signature Algorithm : SHA-1 With RSA Encryption

TCP	443	www	√ 1.0	**Title:** Missing or Permissive X-Frame-Options HTTP Response Header **Synopsis:** The remote web server does not take steps to mitigate a class of web application vulnerabilities. **Impact:** The remote web server in some responses sets a permissive X-Frame-Options response header or does not set one at all. The X-Frame-Options header has been proposed by Microsoft as a way to mitigate clickjacking attacks and is currently supported by all major browser vendors See also : https://en.wikipedia.org/wiki/Clickjacking http://www.nessus.org/u?399b1f56 **Resolution:** Set a properly configured X-Frame-Options header for all requested resources. **Data Received:** The following pages do not set a X-Frame-Options response header or set a permissive policy: - https://global.qwikcast.tv/help
TCP	8172	www	√ 1.0	**Title:** SSL Certificate Information **Synopsis:** This plugin displays the SSL certificate. **Impact:** This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate. **Resolution:** n/a **Data Received:** Subject Name: Country: US State/Province: Washington Locality: Redmond Organization: Microsoft Corporation Common Name: waws-prod-ch1-033.publish.azurewebsites.windows.net Issuer Name: Country: US Organization: DigiCert Inc Common Name: DigiCert SHA2 Secure Server CA Serial Number: 0E 15 AD E1 89 B8 52 98 7F 32 A1 16 D0 A9 FD 0B Version: 3 Signature Algorithm: SHA-256 With RSA Encryption Not Valid Before: Jul 16 00:00:00 2021 GMT Not Valid After: Jul 16 23:59:59 2022 GMT Public Key Info: Algorithm: RSA Encryption Key Length: 2048 bits Public Key: 00 A1 A3 DE 8B 78 9D 53 47 BA 49 B1 A1 F7 41 51 3D DE 5C B7 D3 B2 AA A5 D1 B8 FC 9F 69 29 11 6F D4 E9 62 1E 95 C2 EE AF DD B4 B1 07 4F 53 6E AA A1 DF B7 67 72 CE BA 8B 75 30 16 39 76 AA AE BB D7 52 83 02 B0 DA BC 65 FC AA 21 C2 E3 56 1D F9 DD 74 3D 44 A3 ED F6 66 FE 88 6F FC 6D 18 F4 59 DC D6 3C 2E 68 1B 81 27 32 44 76 A9 C4 36 1C 9F 04 F4 01 28 99 CD 28 2F 22 72 15 09 8E 37 44 67 97 C8 F8 3B 90 7C B7 7B 9F 7A 50 12 1E CB 1B 85 61 AE 9F AF 98 81 54 4F 1D 29 C8 5C E8 50 12 82 0C A5 0C 46 FF 66 12 E9 AB BD 8A 9E 53 55 CA 4D 72 8B 7A 90 97 86 86 E4 FA 06 3D CD 6D C7 E3 78 4D 6A 36 58 00 AA 95 B3 0E B3 09 82 FC 47 5D C1 20 F1 B7 0B DA 16 F2 ED EF B0 DC 19 8F E5 62 E0 46 10 43 65 C7 34 68 67 49 9D A6 3C 14 84 CC D6 AF 3A B5 56 35 96 DB A6 89 6F 24 BB 83 1E 0C 31 A5 Exponent: 01 00 01 Signature Length: 256 bytes / 2048 bits Signature: 00 AE 10 A2 F8 0C E0 87 56 9A 00 4F 9F BF 4C B6 C7 E3 EC F3 15 A6 8C 5B FB 9C 1D 0E AF 2E AE 4E 55 4B A1 7F 24 DE 5A 8E 74 86 CB 39 EB 2F 45 66 61 B5 73 66 6A BF 53 97 D4 FD 61 18 DA 83 BF E6 82 92 7B D8 3D 98 2F 2F 5F 48 B4 D2 BC 5D 88 C4 0E F2 76 B5 48 AC 65 19 CB 3D A1 EF 8C C6 0D DC 9D 70 14 40 03 A7 2D 45 5F A5 1C C0 54 75 A3 0E A1 57 7C 97 63 1C 94 8D 19 61 32 81 8E 45 20 BD EA 35 EA 49 C8 D9 C2 C1 52 59 BD 0E 04 D3 6A C2 A1 D2 D2 FE DB D0 07 3E 70 42 D3 D3 CE 3E 0C 80 41 C5 82 41 16 90 00 DA BA 50 9C 19 69 42 5B DE B9 8D 43 5C AE A0 5B 6C DE EA 9F 5A 8C 4D 47 D6 43 B9 F6 1F 65 8C 9D 4B 3C 74 31 07 A7 06 80 77 9E 0B 79 2B 25 7A 8F AF A5 65 37 FE 71 AF 46 80 B8 C5 00 74 36 E8 7B 09 33 73 2A 3B 0E CE 98 BA 3D 41 4D 4D B4 98 C5 08 98 02 52 76 03 91 43

3C B9 Extension: Authority Key Identifier (2.5.29.35) Critical: 0 Key Identifier: 0F 80 61 1C 82 31 61 D5 2F 28 E7 8D 46 38 B4 2C E1 C6 D9 E2 Extension: Subject Key Identifier (2.5.29.14) Critical: 0 Subject Key Identifier: 1A 8B FA A7 B0 8F BB 65 66 61 37 48 C8 81 22 B1 97 81 32 CC Extension: Subject Alternative Name (2.5.29.17) Critical: 0 DNS: waws-prod-ch1-033.ftp.azurewebsites.windows.net DNS: waws-prod-ch1-033.publish.azurewebsites.windows.net Extension: Key Usage (2.5.29.15) Critical: 1 Key Usage: Digital Signature, Key Encipherment Extension: Extended Key Usage (2.5.29.37) Critical: 0 Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1) Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2) Extension: CRL Distribution Points (2.5.29.31) Critical: 0 URI: http://crl3.digicert.com/DigiCertSHA2SecureServerCA.crl URI: http://crl4.digicert.com/DigiCertSHA2SecureServerCA.crl Extension: Policies (2.5.29.32) Critical: 0 Policy ID #1: 2.23.140.1.2.2 Qualifier ID #1: Certification Practice Statement (1.3.6.1.5.5.7.2.1) CPS URI: http://www.digicert.com/CPS Extension: Authority Information Access (1.3.6.1.5.5.7.1.1) Critical: 0 Method#1: Online Certificate Status Protocol URI: http://ocsp.digicert.com Method#2: Certificate Authority Issuers URI: http://cacerts.digicert.com/DigiCertSHA2SecureServerCA-2.crt Extension: Basic Constraints (2.5.29.19) Critical: 1 Extension: 1.3.6.1.4.1.11129.2.4.2 Critical: 0 Data: 04 82 01 6B 01 69 00 77 00 29 79 BE F0 9E 39 39 21 F0 56 73 9F 63 A5 77 E5 BE 57 7D 9C 60 0A F8 F9 4D 5D 26 5C 25 5D C7 84 00 00 01 7A AF 18 2F 82 00 00 04 03 00 48 30 46 02 21 00 B1 E8 17 80 44 0F B9 04 89 FA A5 AC 74 E8 BC FB 9F 01 EC 66 B8 FD AD 72 DA 65 7F 0E 90 C5 E8 53 02 21 00 B5 A1 EC 47 9A C4 11 34 4B D3 5A 76 FE 6C 52 33 4A 60 C1 8F 7B 07 65 C6 CD 12 3D C7 D1 85 59 0D 00 76 00 51 A3 B0 F5 FD 01 79 9C 56 6D B8 37 78 8F 0C A4 7A CC 1B 27 CB F7 9E 88 42 9A 0D FE D4 8B 05 E5 00 00 01 7A AF 18 2F 87 00 00 04 03 00 47 30 45 02 20 1D DE 5E 98 F7 47 E2 62 EF C3 9C B0 58 D5 D9 21 CC 17 05 95 E5 BD 83 27 8A 79 8A 8A B5 65 79 12 02 21 00 F7 EF 55 2E 46 54 7F 4D 2F 62 A6 BE 7F EE E8 9A 7C CB 61 E8 1D A7 27 1E 39 04 B1 6D E3 3A 95 93 00 76 00 41 C8 CA B1 DF 22 46 4A 10 C6 A1 3A 09 42 87 5E 4E 31 8B 1B 03 EB EB 4B C7 68 F0 90 62 96 06 F6 00 00 01 7A AF 18 2F 3C 00 00 04 03 00 47 30 45 02 20 31 59 95 6D 90 58 5F E0 90 A0 DA 32 7A 49 CF D5 FC 4B A7 7A D6 A3 49 C8 52 82 52 08 77 65 18 E5 02 21 00 84 55 92 91 02 DD 91 A1 20 40 EE D5 51 14 30 07 4E 00 6E 11 AD 7A 79 BB 0C ED 0F A1 5A 31 8A DF Fingerprints : SHA-256 Fingerprint: 19 B3 7B 10 BC C9 42 16 07 BB 2B E0 7B F7 30 E7 9C B7 10 75 28 D4 84 48 2C DD 0A 39 C6 65 AB 71 SHA-1 Fingerprint: E0 31 0F B7 93 92 A7 39 3F 39 A8 3B 78 DA 90 9B 50 8F 52 80 MD5 Fingerprint: 97 22 FF 65 27 6D 28 AA F3 D8 7D BD BD 5B BF E8 PEM certificate : -----BEGIN CERTIFICATE-----
MIIHLDCCBhSgAwIBAgIQDhWt4Ym4Uph/MqEW0Kn9CzANBgkqhkiG9w0BAQsFADBNMQswCQ
YDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMScwJQYDVQQDEx5EaWdpQ2Vyd
CBTSEEyIFNlY3VyZSBTZXJ2ZXIgQ0EwHhcNMjEwNzE2MDAwMDAwWhcNMjIwNzE2MjM1OT
U5WjCBkjELMAkGA1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZ
G1vbmQxHjAcBgNVBAoTFU1pY3Jvc29mdCBDb3Jwb3JhdGlvbjE8MDoGA1UEAxMzd2F3cy1wc
m9kLWNoMS0wMzMucHVibGlzaC5henVyZXdlYnNpdGVzLndpbmRvd3MubmV0MIIBIjANBgkqh
kiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAoaPei3idU0e6SbGh90FRPd5ct9OyqqXRuPyfaSkRb9T
pYh6Vwu6v3bSxB09Tbqqh37dncs66i3UwFjl2qq6711KDArDavGX8qiHC41Yd+d10PUSj7fZm/oh
v/G0Y9Fnc1jwuaBuBJzJEdqnENhyfBPQBKJnNKC8ichUJjjdEZ5fI+DuQfLd7n3pQEh7LG4Vhrp+v
mIFUTx0pyFzoUBKCDKUMRv9mEumrvYqeU1XKTXKLepCXhobk+gY9zW3H43hNajZYAKqVsw6
zCYL8R13BIPG3C9oW8u3vsNwZj+Vi4EYQQ2XHNGhnSZ2mPBSEzNavOrVWNZbbpolvJLuDHg
wxpQIDAQABo4IDwDCCA7wwHwYDVR0jBBgwFoAUD4BhHIIxYdUvKOeNRji0LOHG2eIwHQYDV
R0OBBYEFBqL+qewj7tlZmE3SMiBIrGXgTLMMG8GA1UdEQRoMGaCL3dhd3MtcHJvZC1jaDEtM
DMzLmZ0cC5henVyZXdlYnNpdGVzLndpbmRvd3MubmV0gjN3YXdzLXByb2QtY2gxLTAzMy5wd
WJsaXNoLmF6dXJld2Vic2l0ZXMud2luZG93cy5uZXQwDgYDVR0PAQH/BAQDAgWgMB0GA1U
dJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjCBiAYDVR0fBIGAMH4wPaA7oDmGN2h0dHA
6Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydFNIQTJTZWN1cmVTZXJ2ZXJDQS5jcmwwP
aA7oDmGN2h0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydFNIQTJTZWN1cmVTZX
J2ZXJDQS5jcmwwPgYDVR0gBDcwNTAzBgZngQwBAgIwKTAnBggrBgEFBQcCARYbaHR0cDov
L3d3dy5kaWdpY2VydC5jb20vQ1BTMH4GCCsGAQUFBwEBBHIwcDAkBggrBgEFBQcwAYYYaHR
0cDovL29jc3AuZGlnaWNlcnQuY29tMEgGCCsGAQUFBzAChjxodHRwOi8vY2FjZXJ0cy5kaWdpY
2VydC5jb20vRGlnaUNlcnRSEEyU2VjdXJlU2VydmVyQ0EtMi5jcnQwDAYDVR0TAQH/BAIwADC
CAX8GCisGAQQB1nkCBAIEggFvBIIBawFpAHcAKXm+8J45OSHwVnOfY6V35b5XfZxgCvj5TV0m
XCVdx4QAAAF6rxgvggAABAMASDBGAiEAsegXgEQPuQSJ+qWsdOi8+58B7Ga4/a1y2mV/DpDF
6FMCIQC1oexHmsQRNEvTWnb+bFIzSmDBj3sHZcbNEj3H0YVZDQB2AFGjsPX9AXmcVm24N3i
PDKR6zBsny/eeiEKaDf7UiwXlAAABeq8YL4cAAAQDAEcwRQIgHd5emPdH4mLvw5ywWNXZIc
wXBZXlvYMninmKirVleRICIQD371UuRlR/TS9ipr5/7uiafMth6B2nJx45BLFt4zqVkwB2AEHIyrHfIkZ
KEMahOglCh15OMYsbA+vrS8do8JBilgb2AAABeq8YLzwAAAQDAEcwRQIgMVmVbZBYX+CQoN
oyeknP1fxLp3rWo0nIUoJSCHdlGOUCIQCEVZKRAt2RoSBA7tVRFDAHTgBuEa16ebsM7Q+hWjG
K3zANBgkqhkiG9w0BAQsFAAOCAQEArhCi+Azgh1aaAE+fv0y2x+Ps8xWmjFv7nB0Ory6uTlVLoX8
k3lqOdIbLOesvRWZhtXNmar9Tl9T9YRjag7/mgpJ72D2YLy9fSLTSvF2IxA7ydrVlrGUZyz2h74zG
DdydcBRAA6ctRV+lHMBUdaMOoVd8l2McII0ZYTKBjkUgveo16knI2cLBUlm9DgTTasKh0tL+29A
HPnBC09POPgyAQcWCQRaQANq6UJwZaUJb3rmNQ1yuoFts3uqfWoxNR9ZDufYfZYydSzx0MQ
enBoB3ngt5KyV6j6+lZTf+ca9GgLjFAHQ26HsJM3MqOw7OmLo9QU1NtJjFCJgCUnYDkUM8uQ=

				= -----END CERTIFICATE-----
TCP	80	www	√ 1.0	**Title:** HyperText Transfer Protocol (HTTP) Redirect Information **Synopsis:** The remote web server redirects requests to the root directory. **Impact:** The remote web server issues an HTTP redirect when requesting the root directory of the web server. This plugin is informational only and does not denote a security problem. **Resolution:** Analyze the redirect(s) to verify that this is valid operation for your web server and/or application. **Data Received:** Request : http://global.qwikcast.tv/ HTTP response : HTTP/1.1 301 Moved Permanently Redirect to : https://global.qwikcast.tv/ Redirect type : 30x redirect Note that SecurityMetrics did not receive a 200 OK response from the last examined redirect.
TCP	8172	www	√ 1.0	**Title:** Web Application Cookies Not Marked Secure **Synopsis:** HTTP session cookies might be transmitted in cleartext. **Impact:** The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies. Note that this plugin detects all general cookies missing the 'secure' cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag. See also : https://www.owasp.org/index.php/SecureFlag **Resolution:** Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision. If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data. **Data Received:** The following cookie does not set the secure cookie flag : Name : __RequestVerificationToken Path : / Value : Gu2uT40rfAnxS8Gj-1Eo8leHGTRSxjMboPMJV69sRIFQNFLeS0ETiunNgumUdpabJkwbx9ZP0otMlvhjB9M59x9nFMg1 Domain : Version : 1 Expires : Comment : Secure : 0 Httponly : 1 Port :

TCP	443	www	√ 1.0	**Title:** Web Server Allows Password Auto-Completion **Synopsis:** The 'autocomplete' attribute is not disabled on password fields. **Impact:** The remote web server contains at least one HTML form field that has an input of type 'password' where 'autocomplete' is not set to 'off'. While this does not represent a risk to this web server per se, it does mean that users who use the affected forms may have their credentials saved in their browsers, which could in turn lead to a loss of confidentiality if any of them use a shared host or if their machine is compromised at some point. **Resolution:** Add the attribute 'autocomplete=off' to these fields to prevent browsers from caching credentials. **Data Received:** Page : /Account/Login/loginLink Destination Page: /Account/Login/loginLink Page : /Account/Login Destination Page: /Account/Login
TCP	443	www	√ 1.0	**Title:** Web Server No 404 Error Code Check **Synopsis:** The remote web server does not return 404 error codes. **Impact:** The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page. SecurityMetrics has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate. **Resolution:** n/a **Data Received:** CGI scanning will be disabled for this host because the host responds to requests for non-existent URLs with HTTP code 302 rather than 404. The requested URL was : https://global.qwikcast.tv/0uDW9XPu7RhB.html

TCP	8172	www	√ 1.0	**Title:** SSL Cipher Suites Supported **Synopsis:** The remote service encrypts communications using SSL. **Impact:** This plugin detects which SSL ciphers are supported by the remote service for encrypting communications. See also : https://www.openssl.org/docs/man1.1.0/apps/ciphers.html http://www.nessus.org/u?3a040ada **Resolution:** n/a **Data Received:** Here is the list of SSL ciphers supported by the remote server : Each group is reported per SSL Version. SSL Version : TLSv12 High Strength Ciphers (>= 112-bit key) Name Code KEX Auth Encryption MAC ---------- ---------- --- ---- ---------- --- RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256 RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384 ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1 ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1 AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1 AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1 ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256 ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384 RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256 RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256 The fields above are : {Tenable ciphername} {Cipher ID code} Kex={key exchange} Auth={authentication} Encrypt={symmetric encryption method} MAC={message authentication code} {export flag}
TCP	80	www	√ 1.0	**Title:** Web Server No 404 Error Code Check **Synopsis:** The remote web server does not return 404 error codes. **Impact:** The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page. SecurityMetrics has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate. **Resolution:** n/a **Data Received:** CGI scanning will be disabled for this host because the host responds to requests for non-existent URLs with HTTP code 301 rather than 404. The requested URL was : http://global.qwikcast.tv/0uDW9XPu7RhB.html

TCP	1221	www	√ 1.0	**Title:** Web Server No 404 Error Code Check **Synopsis:** The remote web server does not return 404 error codes. **Impact:** The remote web server is configured such that it does not return '404 Not Found' error codes when a nonexistent file is requested, perhaps returning instead a site map, search page or authentication page. SecurityMetrics has enabled some counter measures for this. However, they might be insufficient. If a great number of security holes are produced for this port, they might not all be accurate. **Resolution:** n/a **Data Received:** Unfortunately, SecurityMetrics has been unable to find a way to recognize this page so some CGI-related checks have been disabled.
TCP	443		√ 1.0	**Title:** Enumerated CGIBIN List **Synopsis:** SecurityMetrics was able to enumerate the following cgibin directories on port 443: /public/Content/themes/base\n1632773050 \n1632773050 /Account\n1632773050 /Account/Login\n1632773050 /public/Content\n1632773050 **Resolution:** No resolution required.
TCP	8172	www	√ 1.0	**Title:** SSL / TLS Versions Supported **Synopsis:** The remote service encrypts communications. **Impact:** This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications. **Resolution:** n/a **Data Received:** This port supports TLSv1.2.

TCP	454	www	√ 1.0	**Title:** SSL Root Certification Authority Certificate Information **Synopsis:** A root Certification Authority certificate was found at the top of the certificate chain. **Impact:** The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain. See also : https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10) **Resolution:** Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies. **Data Received:** The following root Certification Authority certificate was found : |-Subject : C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA |-Issuer : C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA |-Valid From : Nov 10 00:00:00 2006 GMT |-Valid To : Nov 10 00:00:00 2031 GMT |-Signature Algorithm : SHA-1 With RSA Encryption
TCP	8172	www	√ 1.0	**Title:** SSL Certificate 'commonName' Mismatch **Synopsis:** The 'commonName' (CN) attribute in the SSL certificate does not match the hostname. **Impact:** The service running on the remote host presents an SSL certificate for which the 'commonName' (CN) attribute does not match the hostname on which the service listens. **Resolution:** If the machine has several names, make sure that users connect to the service through the DNS hostname that matches the common name in the certificate. **Data Received:** The host name known by SecurityMetrics is : global.qwikcast.tv The Common Name in the certificate is : waws-prod-ch1-033.publish.azurewebsites.windows.net The Subject Alternate Names in the certificate are : waws-prod-ch1-033.ftp.azurewebsites.windows.net waws-prod-ch1-033.publish.azurewebsites.windows.net

TCP	443	www	√ 1.0	**Title:** TLS Version 1.2 Protocol Detection **Synopsis:** The remote service encrypts traffic using a version of TLS. **Impact:** The remote service accepts connections encrypted using TLS 1.2. See also : https://tools.ietf.org/html/rfc5246 **Resolution:** N/A **Data Received:** TLSv1.2 is enabled and the server supports at least one cipher.
TCP		general	√ 1.0	**Title:** Additional DNS Hostnames **Synopsis:** SecurityMetrics has detected potential virtual hosts. **Impact:** Hostnames different from the current hostname have been collected by miscellaneous plugins. SecurityMetrics has generated a list of hostnames that point to the remote host. Note that these are only the alternate hostnames for vhosts discovered on a web server. Different web servers may be hosted on name-based virtual hosts. See also : https://en.wikipedia.org/wiki/Virtual_hosting **Resolution:** If you want to test them, re-scan using the special vhost syntax, such as : www.example.com[192.0.32.10] **Data Received:** The following hostnames point to the remote host : - waws-prod-ch1-033.api.azurewebsites.windows.net

TCP	443	www	√ 1.0	**Title:** HSTS Missing From HTTPS Server **Synopsis:** The remote web server is not enforcing HSTS. **Impact:** The remote HTTPS server is not enforcing HTTP Strict Transport Security (HSTS). HSTS is an optional response header that can be configured on the server to instruct the browser to only communicate via HTTPS. The lack of HSTS allows downgrade attacks, SSL-stripping man-in-the-middle attacks, and weakens cookie-hijacking protections. See also : https://tools.ietf.org/html/rfc6797 **Resolution:** Configure the remote web server to use HSTS. For Nginx see: https://www.nginx.com/blog/http-strict-transport-security-hsts-and-nginx/ For Apache see: https://linux-audit.com/configure-hsts-http-strict-transport-security-apache-nginx/ Microsoft Azure/ISS: https://docs.microsoft.com/en-us/azure/frontdoor/front-door-security-headers https://docs.microsoft.com/en-us/iis/configuration/system.applicationhost/sites/site/hsts General: https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html https://https.cio.gov/hsts/ **Data Received:** The remote HTTPS server does not send the HTTP "Strict-Transport-Security" header.
TCP	1221	www	√ 1.0	**Title:** GitLab Web UI Detection **Synopsis:** GitLab Web UI Detection. **Impact:** GitLab web user interface detected on remote host. GitLab is a web-based DevOps lifecycle tool that provides a Git repository manager providing wiki, issue-tracking and continuous integration and deployment pipeline features, using an open-source license, developed by GitLab Inc. **Resolution:** n/a **Data Received:** URL : http://global.qwikcast.tv:1221/ Version : unknown

TCP	443	www	√ 1.0	**Title:** SSL Cipher Suites Supported **Synopsis:** The remote service encrypts communications using SSL. **Impact:** This plugin detects which SSL ciphers are supported by the remote service for encrypting communications. See also : https://www.openssl.org/docs/man1.1.0/apps/ciphers.html http://www.nessus.org/u?3a040ada **Resolution:** n/a **Data Received:** Here is the list of SSL ciphers supported by the remote server : Each group is reported per SSL Version. SSL Version : TLSv12 High Strength Ciphers (>= 112-bit key) Name Code KEX Auth Encryption MAC ---------- ---------- --- ---- ---------- --- ECDHE-RSA-AES128-SHA256 0xC0, 0x2F ECDH RSA AES-GCM(128) SHA256 ECDHE-RSA-AES256-SHA384 0xC0, 0x30 ECDH RSA AES-GCM(256) SHA384 RSA-AES128-SHA256 0x00, 0x9C RSA RSA AES-GCM(128) SHA256 RSA-AES256-SHA384 0x00, 0x9D RSA RSA AES-GCM(256) SHA384 ECDHE-RSA-AES128-SHA 0xC0, 0x13 ECDH RSA AES-CBC(128) SHA1 ECDHE-RSA-AES256-SHA 0xC0, 0x14 ECDH RSA AES-CBC(256) SHA1 AES128-SHA 0x00, 0x2F RSA RSA AES-CBC(128) SHA1 AES256-SHA 0x00, 0x35 RSA RSA AES-CBC(256) SHA1 ECDHE-RSA-AES128-SHA256 0xC0, 0x27 ECDH RSA AES-CBC(128) SHA256 ECDHE-RSA-AES256-SHA384 0xC0, 0x28 ECDH RSA AES-CBC(256) SHA384 RSA-AES128-SHA256 0x00, 0x3C RSA RSA AES-CBC(128) SHA256 RSA-AES256-SHA256 0x00, 0x3D RSA RSA AES-CBC(256) SHA256 The fields above are : {Tenable ciphername} {Cipher ID code} Kex={key exchange} Auth={authentication} Encrypt={symmetric encryption method} MAC={message authentication code} {export flag}
TCP	1221	www	√ 1.0	**Title:** Non-compliant Strict Transport Security (STS) **Synopsis:** The remote web server implements Strict Transport Security incorrectly. **Impact:** The remote web server implements Strict Transport Security. However, it does not respect all the requirements of the STS draft standard. See also : http://www.nessus.org/u?2fb3aca6 **Resolution:** n/a **Data Received:** The Strict-Transport-Security header must not be sent over an unencrypted channel.

TCP	443	www	√ 1.0	**Title:** OpenSSL Detection **Synopsis:** The remote service appears to use OpenSSL to encrypt traffic. **Impact:** Based on its response to a TLS request with a specially crafted server name extension, it seems that the remote service is using the OpenSSL library to encrypt traffic. Note that this plugin can only detect OpenSSL implementations that have enabled support for TLS extensions (RFC 4366). See also : https://www.openssl.org/ **Resolution:** n/a
TCP	1221	www	√ 1.0	**Title:** Strict Transport Security (STS) Detection **Synopsis:** The remote web server implements Strict Transport Security. **Impact:** The remote web server implements Strict Transport Security (STS). The goal of STS is to make sure that a user does not accidentally downgrade the security of his or her browser. All unencrypted HTTP connections are redirected to HTTPS. The browser is expected to treat all cookies as 'secure' and to close the connection in the event of potentially insecure situations. See also : http://www.nessus.org/u?2fb3aca6 **Resolution:** n/a **Data Received:** The STS header line is : Strict-Transport-Security: max-age=31536000
TCP	443	www	√ 1.0	**Title:** SSL Certificate Information **Synopsis:** This plugin displays the SSL certificate. **Impact:** This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate. **Resolution:** n/a **Data Received:** Subject Name: Organization Unit: Domain Control Validated Common Name: *.qwikcast.tv Issuer Name: Country: US State/Province: Arizona Locality: Scottsdale Organization: GoDaddy.com, Inc. Organization Unit: http://certs.godaddy.com/repository/ Common Name: Go Daddy Secure Certificate Authority - G2 Serial Number: 00 81 44 A6 0F F1 46 8A 03 Version: 3 Signature Algorithm: SHA-256 With RSA Encryption Not Valid Before: Jul 21 07:03:54 2020 GMT Not Valid After: Jul 28 21:20:39 2022 GMT Public Key Info: Algorithm: RSA Encryption Key Length: 2048 bits Public Key: 00 C3 A3 CC 46 FC 98 C4 F3 27 32 D0 91 42 7D A7 31 FD 20 5C 04 86 33 EC B1 C0 7F 02 E4 44 19 FE 88 CD 7D 00 9C 79 F2 4F AC C8 A1 ED 2D E2 BA E3 C0 92 42 3F BE 88 78 D4 18 79 CB AA 42 62 EF EE 80 18 40 E5 20 87 A0 48 77 FC 53 E7 F6 41 9F 8E D4 9C FA 89 A4 69 12 08 3D 19 06 69 42 5C 1A C7 4E 59 38 A6 96 3D AB 6E 91 87 37

86 7D 3D 19 49 E7 9F A6 F3 D9 CC EC A4 97 DB 08 4F 0A 27 01 C5 29 FA 2B 15 57 6F 07 C5 C1 0F 6B FC FC B6 7F 21 22 54 C2 A2 77 87 8A A3 A2 50 89 EE 19 F9 4A 94 3D B2 49 71 39 40 E3 E8 B1 0A D2 04 A8 C7 92 32 4B 00 BF D7 67 05 DD B5 E3 AD D4 9C B7 32 3E D1 ED 40 19 AE 86 86 78 5A F1 83 55 42 36 40 0F 16 BD 56 9E 75 FA 54 50 15 06 1B 08 AD 33 43 F9 FB D6 11 1E 43 59 3F D9 68 A0 E5 94 31 FF 1D 80 1C 61 D8 BE AA 70 EB 3E AC 8F C2 DA 6B 0B 51 37 19 43 Exponent: 01 00 01 Signature Length: 256 bytes / 2048 bits Signature: 00 15 D2 53 30 E6 97 95 A7 59 30 46 26 29 6E 35 36 7E ED 27 2E 85 38 52 A1 14 4F 8E 54 8D FE 7F AE C2 2F 5D EA 93 14 7B 0D EB 73 ED C1 CB 85 05 8A 02 12 4F 77 88 59 CA 18 10 12 98 AD 9C 43 EC 29 E1 7A 5A 50 41 9A 92 1D 1B F7 75 26 82 26 29 30 5C E0 EF A5 BE B6 66 CE 9D CB 5D 74 B8 76 26 25 2F 6D 41 95 79 0A 13 07 2F DC 4F 74 37 29 E2 C7 B5 CA AB D3 47 74 6D 0D D7 13 A5 54 8F E6 9B 13 B8 12 BD D0 5C 10 DB 56 FB 1F 6B BC 4E DA 64 AF 55 58 77 B1 A6 5B 8F 28 4F F2 C8 23 B7 63 F6 8A 75 97 18 8C 61 75 DF 09 30 5B 79 AB 7B 4B 41 D3 04 5B 1D C4 58 50 94 13 1C 25 B1 A0 37 97 F0 14 47 96 A7 31 E0 99 A3 68 9E 76 C0 A8 8B 2F A1 93 27 F2 27 C0 9E 6D 64 02 BB A4 F2 CE D0 50 56 4D 9E D8 8E 32 3E E5 BB 07 B5 BD 17 DF 6A 05 60 9C 64 23 31 DE 10 25 CB 35 EA E3 90 59 5E 34 8E 2A Extension: Basic Constraints (2.5.29.19) Critical: 1 Extension: Extended Key Usage (2.5.29.37) Critical: 0 Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1) Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2) Extension: Key Usage (2.5.29.15) Critical: 1 Key Usage: Digital Signature, Key Encipherment Extension: CRL Distribution Points (2.5.29.31) Critical: 0 URI: http://crl.godaddy.com/gdig2s1-2140.crl Extension: Policies (2.5.29.32) Critical: 0 Policy ID #1: 2.16.840.1.114413.1.7.23.1 Qualifier ID #1: Certification Practice Statement (1.3.6.1.5.5.7.2.1) CPS URI: http://certificates.godaddy.com/repository/ Policy ID #2: 2.23.140.1.2.1 Extension: Authority Information Access (1.3.6.1.5.5.7.1.1) Critical: 0 Method#1: Online Certificate Status Protocol URI: http://ocsp.godaddy.com/ Method#2: Certificate Authority Issuers URI: http://certificates.godaddy.com/repository/gdig2.crt Extension: Authority Key Identifier (2.5.29.35) Critical: 0 Key Identifier: 40 C2 BD 27 8E CC 34 83 30 A2 33 D7 FB 6C B3 F0 B4 2C 80 CE Extension: Subject Alternative Name (2.5.29.17) Critical: 0 DNS: *.qwikcast.tv DNS: qwikcast.tv Extension: Subject Key Identifier (2.5.29.14) Critical: 0 Subject Key Identifier: E4 E7 CF B2 90 60 4B E2 DB 25 48 E4 E5 60 0C F8 84 06 83 D0 Extension: 1.3.6.1.4.1.11129.2.4.2 Critical: 0 Data: 04 82 01 6B 01 69 00 76 00 29 79 BE F0 9E 39 39 21 F0 56 73 9F 63 A5 77 E5 BE 57 7D 9C 60 0A F8 F9 4D 5D 26 5C 25 5D C7 84 00 00 01 73 70 2F 9D 1A 00 00 04 03 00 47 30 45 02 20 15 96 0B AA 7C 2E 39 47 27 59 44 D6 D6 B3 71 40 9F 9A 29 B8 C4 F9 63 F6 61 03 84 36 FA 7C 46 48 02 21 00 B7 2B 26 B7 8C 5C 3B 46 6C 82 AD D5 7A D9 45 FE 5B C3 C5 74 C5 03 CA 81 AA FF 7D 34 FC 47 DE A7 00 77 00 22 45 45 07 59 55 24 56 96 3F A1 2F F1 F7 6D 86 E0 23 26 63 AD C0 4B 7F 5D C6 83 5C 6E E2 0F 02 00 00 01 73 70 2F 9E 62 00 00 04 03 00 48 30 46 02 21 00 86 0B 06 1F 19 B4 23 3D 5B B1 E3 B4 B3 EA DE 80 70 85 AF 5F E5 34 1A 94 5C B5 7D D7 17 1E 45 2E 02 21 00 E5 E5 7B FD 73 C3 E5 CE 97 6A 8C F7 EF BE FD E4 89 24 71 23 1F 91 15 B9 03 B6 D8 92 AC B2 39 A9 00 76 00 DF A5 5E AB 68 82 4F 1F 6C AD EE B8 5F 4E 3E 5A EA CD A2 12 A4 6A 5E 8E 3B 12 C0 20 44 5C 2A 73 00 00 01 73 70 2F 9F AA 00 00 04 03 00 47 30 45 02 20 2A 55 31 05 AE 9A 8D AB 9D FF FA BC 45 4B B1 D6 53 8E B4 95 2D 93 74 87 CD 5F A5 5D BD F6 26 02 02 21 00 E8 03 7E D3 B7 F9 B3 05 90 BF 94 78 A2 EE 18 F9 40 FA E0 84 CA C9 FE D8 6A 51 8B 25 4D E8 FD A1 Fingerprints : SHA-256 Fingerprint: 86 20 07 12 CC A5 78 AE 3F 59 9D 95 46 6E 05 60 1A C8 DA 7C BC B5 22 BE 38 77 CF BD BA C9 31 A4 SHA-1 Fingerprint: 00 D3 17 EB 26 17 C8 1C C7 1C FF D4 9A B9 94 FA FA 82 55 05 MD5 Fingerprint: 45 5B 5E A6 FF 02 D0 67 F3 3E 57 A4 A7 6E 17 E9 PEM certificate : -----BEGIN CERTIFICATE-----

MIIGsTCCBZmgAwIBAgIJAIFEpg/xRooDMA0GCSqGSIb3DQEBCwUAMIG0MQswCQYDVQQGEw
JVUzEQMA4GA1UECBMHQXJpem9uYTETMBEGA1UEBxMKU2NvdHRzZGFsZTEaMBgGA1UEC
hMRR29EYWRkeS5jb20sIEluYy4xLTArBgNVBAsTJGh0dHA6Ly9jZXJ0cy5nb2RhZGR5LmNvbS9
yZXBvc2l0b3J5LzEzMDEGA1UEAxMqR28gRGFkZHkgU2VjdXJlIENlcnRpZmljYXRlIEF1dGhvcml0
eSAtIEcyMB4XDTIwMDcyMTA3MDM1NFoXDTIyMDcyODIxMjAzOVowOzEhMB8GA1UECxMYR
G9tYWluIENvbnRyb2wgVmFsaWRhdGVkMRYwFAYDVQQDDA0qLnF3aWtjYXN0LnR2MIIBIjANB
gkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAw6PMRvyYxPMnMtCRQn2nMf0gXASGM+yxwH8
C5EQZ/ojNfQCcefJPrMih7S3iuuPAkkI/voh41Bh5y6pCYu/ugBhA5SCHoEh3/FPn9kGfjtSc+omkaR
IIPRkGaUJcGsdOWTimlj2rbpGHN4Z9PRlJ55+m89nM7KSX2whPCicBxSn6KxVXbwfFwQ9r/Py2f
yEiVMKid4eKo6JQie4Z+UqUPbJJcTlA4+ixCtIEqMeSMksAv9dnBd21463UnLcyPtHtQBmuhoZ4
WvGDVUI2QA8WvVaedfpUUBUGGwitM0P5+9YRHkNZP9looOWUMf8dgBxh2L6qcOs+rI/C2msL
UTcZQwIDAQABo4IDPDCCAzgwDAYDVR0TAQH/BAIwADAdBgNVHSUEFjAUBggrBgEFBQcDAQ
YIKwYBBQUHAwIwDgYDVR0PAQH/BAQDAgWgMDgGA1UdHwQxMC8wLaAroCmGJ2h0dHA6L
y9jcmwuZ29kYWRkeS5jb20vZ2RpZzJzMS0yMTQwLmNybDBdBgNVHSAEVjBUMEgGC2CGSA
GG/W0BBxcBMDkwNwYIKwYBBQUHAgEWK2h0dHA6Ly9jZXJ0aWZpY2F0ZXMuZ29kYWRkeS
5jb20vcmVwb3NpdG9yeS8wCAYGZ4EMAQIBMHYGCCsGAQUFBwEBBGowaDAkBggrBgEFBQc
wAYYYaHR0cDovL29jc3AuZ29kYWRkeS5jb20vMEAGCCsGAQUFBzAChjRodHRwOi8vY2VydGl
maWNhdGVzLmdvZGFkZHkuY29tL3JlcG9zaXRvcnkvZ2RpZzIuY3J0MB8GA1UdIwQYMBaAFED
CvSeOzDSDMKIz1/tss/C0LIDOMCUGA1UdEQQeMByCDSoucXdpa2Nhc3QudHaCC3F3aWtjYXN
0LnR2MB0GA1UdDgQWBBTk58+ykGBL4tslSOTlYAz4hAaD0DCCAX8GCisGAQQB1nkCBAIEggF
vBIIBawFpAHYAKXm+8J45OSHwVnOfY6V35b5XfZxgCvj5TV0mXCVdx4QAAAFzcC+dGgAABAM

				ARzBFAiAVlguqfC45RydZRNbWs3FAn5opuMT5Y/ZhA4Q2+nxGSAIhALcrJreMXDtGbIKt1XrZRf5bw8V0xQPKgar/fTT8R96nAHcAIkVFB1IVJFaWP6Ev8fdthuAjJmOtwEt/XcaDXG7iDwIAAAFzcC+eYgAABAMASDBGAiEAhgsGHxm0Iz1bseO0s+regHCFr1/lNBqUXLV91xceRS4CIQDI5Xv9c8PlzpdqjPfvvv3kiSRxIx+RFbkDttiSrLI5qQB2AN+IXqtogk8fbK3uuF9OPlrqzaISpGpejjsSwCBEXCpzAAABc3Avn6oAAAQDAEcwRQIgKlUxBa6ajaud//q8RUux1lOOtJUtk3SHzV+lXb32JgICIQDoA37Tt/mzBZC/lHii7hj5QPrghMrJ/thqUYslTej9oTANBgkqhkiG9w0BAQsFAAOCAQEAFdJTMOaXladZMEYmKW41Nn7tJy6FOFKhFE+OVI3+f67CL13qkxR7Detz7cHLhQWKAhJPd4hZyhgQEpitnEPsKeF6WlBBmpIdG/d1JoImKTBc4O+lvrZmzp3LXXS4diYlL21BlXkKEwcv3E90Nynix7XKq9NHdG0N1xOlVl/mmxO4Er3QXBDbVvsfa7xO2mSvVVh3saZbjyhP8sgjt2P2inWXGIxhdd8JMFt5q3tLQdMEWx3EWFCUExwIsaA3l/AUR5anMeCZo2iedsCoiy+hkyfyJ8CebWQCu6TyztBQVk2e2I4yPuW7B7W9F99qBWCcZCMx3hAlyzXq45BZXjSOKg== -----END CERTIFICATE-----
TCP	454	www	√ 1.0	**Title:** SSL / TLS Versions Supported **Synopsis:** The remote service encrypts communications. **Impact:** This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications. **Resolution:** n/a **Data Received:** This port supports TLSv1.2.
TCP	8172	www	√ 1.0	**Title:** SSL Root Certification Authority Certificate Information **Synopsis:** A root Certification Authority certificate was found at the top of the certificate chain. **Impact:** The remote service uses an SSL certificate chain that contains a self-signed root Certification Authority certificate at the top of the chain. See also : https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc778623(v=ws.10) **Resolution:** Ensure that use of this root Certification Authority certificate complies with your organization's acceptable use and security policies. **Data Received:** The following root Certification Authority certificate was found : |-Subject : C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA |-Issuer : C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root CA |-Valid From : Nov 10 00:00:00 2006 GMT |-Valid To : Nov 10 00:00:00 2031 GMT |-Signature Algorithm : SHA-1 With RSA Encryption

TCP	1221	www	√ 1.0	**Title:** SonicWall Secure Mobile Access (SMA) Web Detection **Synopsis:** The web interface for a remote access device was detected on the remote host. **Impact:** The remote host is a SonicWall Secure Mobile Access (SMA) or Secure Remote Access (SRA) device. It is possible to obtain the version and model via the web interface. Note that HTTP form credentials may be required to retrieve the model information. **Resolution:** n/a **Data Received:** URL : http://global.qwikcast.tv:1221/ Version : unknown Model : unknown Product : SonicWall Secure Mobile Access
TCP	443	www	√ 1.0	**Title:** Web Application Sitemap **Synopsis:** The remote web server hosts linkable content that can be crawled by SecurityMetrics. **Impact:** The remote web server contains linkable content that can be used to gather information about a target. See also : http://www.nessus.org/u?5496c8d9 **Resolution:** n/a **Data Received:** The following sitemap was created from crawling linkable content on the target host : - https://global.qwikcast.tv/ - https://global.qwikcast.tv/Account/Login - https://global.qwikcast.tv/Account/Login/loginLink - https://global.qwikcast.tv/Account/_ForgotPassword - https://global.qwikcast.tv/Areas/HelpPage/HelpPage.css - https://global.qwikcast.tv/favicon.ico - https://global.qwikcast.tv/help - https://global.qwikcast.tv/home - https://global.qwikcast.tv/public/Content/SiteBundle - https://global.qwikcast.tv/public/Content/groundworkBundle - https://global.qwikcast.tv/public/Content/spectrumBundle - https://global.qwikcast.tv/public/Content/themes/base/partialpageBundle Attached is a copy of the sitemap file.

TCP	454	www	√ 1.0	**Title:** Web Application Cookies Not Marked Secure **Synopsis:** HTTP session cookies might be transmitted in cleartext. **Impact:** The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies. Note that this plugin detects all general cookies missing the 'secure' cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag. See also : https://www.owasp.org/index.php/SecureFlag **Resolution:** Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision. If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data. **Data Received:** The following cookie does not set the secure cookie flag : Name : __RequestVerificationToken Path : / Value : Gu2uT40rfAnxS8Gj-1Eo8leHGTRSxjMboPMJV69sRIFQNFLeS0ETiunNgumUdpabJkwbx9ZP0otMlvhjB9M59x9nFMg1 Domain : Version : 1 Expires : Comment : Secure : 0 Httponly : 1 Port :
TCP	443	www	√ 1.0	**Title:** Web Application Cookies Not Marked Secure **Synopsis:** HTTP session cookies might be transmitted in cleartext. **Impact:** The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies. Note that this plugin detects all general cookies missing the 'secure' cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag. See also : https://www.owasp.org/index.php/SecureFlag **Resolution:** Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision. If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data. **Data Received:** The following cookie does not set the secure cookie flag : Name : __RequestVerificationToken Path : / Value : Gu2uT40rfAnxS8Gj-1Eo8leHGTRSxjMboPMJV69sRIFQNFLeS0ETiunNgumUdpabJkwbx9ZP0otMlvhjB9M59x9nFMg1 Domain : Version : 1 Expires : Comment : Secure : 0 Httponly : 1 Port :

TCP	80	www	√ 1.0	**Title:** Web Application Cookies Not Marked Secure **Synopsis:** HTTP session cookies might be transmitted in cleartext. **Impact:** The remote web application sets various cookies throughout a user's unauthenticated and authenticated session. However, there are instances where the application is running over unencrypted HTTP or the cookies are not marked 'secure', meaning the browser could send them back over an unencrypted link under certain circumstances. As a result, it may be possible for a remote attacker to intercept these cookies. Note that this plugin detects all general cookies missing the 'secure' cookie flag, whereas plugin 49218 (Web Application Session Cookies Not Marked Secure) will only detect session cookies from an authenticated session missing the secure cookie flag. See also : https://www.owasp.org/index.php/SecureFlag **Resolution:** Each cookie should be carefully reviewed to determine if it contains sensitive data or is relied upon for a security decision. If possible, ensure all communication occurs over an encrypted channel and add the 'secure' attribute to all session cookies or any cookies containing sensitive data. **Data Received:** The following cookie does not set the secure cookie flag : Name : __RequestVerificationToken Path : / Value : Gu2uT40rfAnxS8Gj-1Eo8leHGTRSxjMboPMJV69sRIFQNFLeS0ETiunNgumUdpabJkwbx9ZP0otMlvhjB9M59x9nFMg1 Domain : Version : 1 Expires : Comment : Secure : 0 Httponly : 1 Port :
TCP	454	www	√ 1.0	**Title:** SSL Certificate Information **Synopsis:** This plugin displays the SSL certificate. **Impact:** This plugin connects to every SSL-related port and attempts to extract and dump the X.509 certificate. **Resolution:** n/a **Data Received:** Subject Name: Country: US State/Province: Washington Locality: Redmond Organization: Microsoft Corporation Common Name: waws-prod-ch1-033.api.azurewebsites.windows.net Issuer Name: Country: US Organization: DigiCert Inc Common Name: DigiCert SHA2 Secure Server CA Serial Number: 09 28 9F F0 D4 0E DF 90 14 88 37 AF FA 9B E3 38 Version: 3 Signature Algorithm: SHA-256 With RSA Encryption Not Valid Before: Jul 13 00:00:00 2021 GMT Not Valid After: Jul 13 23:59:59 2022 GMT Public Key Info: Algorithm: RSA Encryption Key Length: 2048 bits Public Key: 00 C7 68 08 63 87 B6 6C 1F BE AC 4B CF 5C 56 47 83 70 10 3D DC 78 AF 6E 8F 4A 61 09 9E F3 B1 8E B1 12 C4 C3 CE 31 D9 A4 6F 62 FA 4D 5D E8 EA 93 5C C0 8B 54 42 25 B7 29 E8 60 8A D5 5C A5 49 13 25 F4 E8 8D A1 B6 CE 58 4B 3D 65 9E CC B7 CF 54 02 63 94 92 38 A2 5A 7C 80 BA 69 42 02 79 DD 1A EE B6 0F D2 F6 21 D7 FB 05 0E CC A1 83 6D D3 67 4A EB F2 1F 86 5A 1B 07 7F 95 DE 90 18 89 2A A8 90 9B 46 BD CA 0C AD 47 45 51 BB F2 6D 48 77 11 36 08 29 05 9E 55 FD FD 89 1F CA F8 25 8D 65 50 E9 FB 66 C3 11 FC A5 C2 E3 74 E9 6C 4F 4C 57 7A D5 F3 EE 9B D6 5A A0 2D CE 2C C6 5F EB B8 86 BD E7 FB 91 FC EC 11 C5 11 B6 DA 4E 0D BD A2 0B FA 68 40 5B A0 39 3B 12 AA 62 74 6A 7D E8 C2 E4 1B 4C E5 4E C5 27 DD 70 D5 CF 7C F5 F4 B5 66 04 D5 FA F5 98 3E F2 C1 11 0E 3C 88 D8 08 4F 74 C0 F3 05 Exponent: 01 00 01 Signature Length: 256 bytes / 2048 bits Signature: 00 55 D1 25 A1 14 12 64 C7 F5 72 69 F4 1A 9A C8 79 0E 95 29 93 BC 84 21 56 C3 57 6D 02 84 D9

				2E DD C5 F3 82 39 9B BA DA FA AE 75 D0 71 FA 28 CA BF 07 61 CB 82 C2 9C FC 85 31 C2 1D 26 B9 E3 0C 6C 44 95 F6 2D FB F5 2D 25 47 ED E7 09 AB 09 59 EB B5 CF 39 BF 80 D9 9B A7 4C E3 0C 0B 5B 49 82 22 FD FC EC E1 88 81 E8 45 36 A5 46 A4 2F 0D BA 46 EB 85 EE 72 C9 CA 27 FC AA 27 09 66 1E 4E EE 08 F6 EF 02 76 FC E1 2A 9C 28 7E 3A 57 0B 1F 6F 30 19 41 19 2A 74 5E 2F A5 87 E1 04 C9 BF 28 87 B6 36 2C E1 F7 02 F3 C9 5C 3D 33 19 08 8D CB 2E 3D 2F F6 67 07 62 BA F8 B5 67 4E 5B 23 DA E3 84 FC BD 25 5F 69 52 15 85 B5 55 27 6F 8E 79 40 10 80 0C EB BD 05 A9 E0 A8 61 52 32 D6 9A E5 2F 57 5E 58 EC AF 09 3D 6F A3 73 98 FE E1 B1 FC 1F 97 EA 64 1F 0D E1 FC 3F 19 E8 6C 7B BA FE 0C 8E 92 05 Extension: Authority Key Identifier (2.5.29.35) Critical: 0 Key Identifier: 0F 80 61 1C 82 31 61 D5 2F 28 E7 8D 46 38 B4 2C E1 C6 D9 E2 Extension: Subject Key Identifier (2.5.29.14) Critical: 0 Subject Key Identifier: BF 49 38 97 E9 10 A1 EF E8 42 4E E7 C7 42 0A AF 0F AE E5 3A Extension: Subject Alternative Name (2.5.29.17) Critical: 0 DNS: waws-prod-ch1-033.api.azurewebsites.windows.net Extension: Key Usage (2.5.29.15) Critical: 1 Key Usage: Digital Signature, Key Encipherment Extension: Extended Key Usage (2.5.29.37) Critical: 0 Purpose#1: Web Server Authentication (1.3.6.1.5.5.7.3.1) Purpose#2: Web Client Authentication (1.3.6.1.5.5.7.3.2) Extension: CRL Distribution Points (2.5.29.31) Critical: 0 URI: http://crl3.digicert.com/DigiCertSHA2SecureServerCA.crl URI: http://crl4.digicert.com/DigiCertSHA2SecureServerCA.crl Extension: Policies (2.5.29.32) Critical: 0 Policy ID #1: 2.23.140.1.2.2 Qualifier ID #1: Certification Practice Statement (1.3.6.1.5.5.7.2.1) CPS URI: http://www.digicert.com/CPS Extension: Authority Information Access (1.3.6.1.5.5.7.1.1) Critical: 0 Method#1: Online Certificate Status Protocol URI: http://ocsp.digicert.com Method#2: Certificate Authority Issuers URI: http://cacerts.digicert.com/DigiCertSHA2SecureServerCA-2.crt Extension: Basic Constraints (2.5.29.19) Critical: 1 Fingerprints : SHA-256 Fingerprint: 6A E3 60 DE 93 3A C2 5F CD 54 B1 99 57 8C 36 3E 6B 50 DB EE B8 72 4F 44 78 A7 4B 92 31 88 7B C9 SHA-1 Fingerprint: A5 7E 53 A0 7C 2A 3A E6 9E C2 C7 4B 29 7A 37 E5 0A A9 79 91 MD5 Fingerprint: 3C 3A 00 76 46 5F DF FF F6 A4 92 55 72 46 83 7A PEM certificate : -----BEGIN CERTIFICATE----- MIIFcDCCBFigAwIBAgIQCSif8NQO35AUiDev+pvjODANBgkqhkiG9w0BAQsFADBNMQswCQYDV QQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMScwJQYDVQQDEx5EaWdpQ2VydCBT SEEyIFNlY3VyZSBTZXJ2ZXIgQ0EwHhcNMjEwNzEzMDAwMDAwWhcNMjIwNzEzMjM1OTU5Wj CBjjELMAkGA1UEBhMCVVMxEzARBgNVBAgTCldhc2hpbmd0b24xEDAOBgNVBAcTB1JlZG1vb mQxHjAcBgNVBAoTFU1pY3Jvc29mdCBDb3Jwb3JhdGlvbjE4MDYGA1UEAxMvd2F3cy1wcm9k LWNoMS0wMzMuYXBpLmF6dXJld2Vic2l0ZXMud2luZG93cy5uZXQwggEiMA0GCSqGSIb3DQE BAQUAA4IBDwAwggEKAoIBAQDHaAhjh7ZsH76sS89cVkeDcBA93Hivbo9KYQme87GOsRLEw8 4x2aRvYvpNXejqk1zAi1RCJbcp6GCK1VylSRMl9OiNobbOWEs9ZZ7Mt89UAmOUkjiWnyAumlCA nndGu62D9L2Idf7BQ7MoYNt02dK6/IfhlobB3+V3pAYiSqokJtGvcoMrUdFUbvybUh3ETYIKQWeVf 39iR/K+CWNZVDp+2bDEfylwuN06WxPTFd61fPum9ZaoC3OLMZf67iGvef7kfzsEcURttpODb2iC/ poQFugOTsSqmJ0an3owuQbTOVOxSfdcNXPfPX0tWYE1fr1mD7ywREOPIjYCE90wPMFAgMBA AGjggIIMIICBDAfBgNVHSMEGDAWgBQPgGEcgjFh1S8o541GOLQs4cbZ4jAdBgNVHQ4EFgQUv0 k4l+kQoe/oQk7nx0IKrw+u5TowOgYDVR0RBDMwMYIvd2F3cy1wcm9kLWNoMS0wMzMuYXBp LmF6dXJld2Vic2l0ZXMud2luZG93cy5uZXQwggDgYDVR0PAQH/BAQDAgWgMB0GA1UdJQQWM BQGCCsGAQUFBwMBBggrBgEFBQcDAjCBiAYDVR0fBIGAMH4wPaA7oDmGN2h0dHA6Ly9jcm wzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydFNlQTJTZWN1cmVTZXJ2ZXJDQS5jcmwwPaA7oDm GN2h0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydFNlQTJTZWN1cmVTZXJ2ZXJDQ S5jcmwwPgYDVR0gBDcwNTAzBgZngQwBAgIwKTAnBggrBgEFBQcCARYbaHR0cDovL3d3dy5k aWdpY2VydC5jb20vQ1BTMH4GCCsGAQUFBwEBBHIwcDAkBggrBgEFBQcwAYYYaHR0cDovL2 9jc3AuZGlnaWNlcnQuY29tMEgGCCsGAQUFBzAChjxodHRwOi8vY2FjZXJ0cy5kaWdpY2VydC5jb 20vRGlnaUNlcnRSEEyU2VjdXJlU2VydmVyQ0EtMi5jcnQwDAYDVR0TAQH/BAIwADANBgkqhki G9w0BAQsFAAOCAQEAVdEloRQSZMf1cmn0GprIeQ6VKZO8hCFWw1dtAoTZLt3F84I5m7ra+q5 10HH6KMq/B2HLgsKc/IUxwh0mueMMbESV9i379S0lR+3nCasJWeu1zzm/gNmbp0zjDAtbSYIi/ fzs4YiB6EU2pUakLw26RuuF7nLJyif8qicJZh5O7gj27wJ2/OEqnCh+OlcLH28wGUEZKnReL6WH 4QTJvyiHtjYs4fcC88lcPTMZCI3LLj0v9mcHYrr4tWdOWyPa44T8vSVfaVIVhbVVJ2+OeUAQgAzrv QWp4KhhUjLWmuUvV15Y7K8JPW+jc5j+4bH8H5fqZB8N4fw/Gehse7r+DI6SBQ== -----END CERTIFICATE-----

TCP	443	www	√ 1.0	**Title:** SSL / TLS Versions Supported **Synopsis:** The remote service encrypts communications. **Impact:** This plugin detects which SSL and TLS versions are supported by the remote service for encrypting communications. **Resolution:** n/a **Data Received:** This port supports TLSv1.2.
TCP	443	www	√ 1.0	**Title:** Microsoft .NET Handlers Enumeration **Synopsis:** It is possible to enumerate the remote .NET handlers used by the remote web server. **Impact:** It is possible to obtain the list of handlers the remote ASP.NET web server supports. See also : https://support.microsoft.com/en-us/help/815145 **Resolution:** None **Data Received:** The remote extensions are handled by the remote ASP.NET server : - .ashx - .aspx - .asmx - .rem - .soap