Scan summary: **ampluart.ru**
01 Aug 21

medium

Thread level

Medium severity bugs allow attackers to read or modify limited amounts of information, or are not harmful on their own but potentially harmful when combined with other bugs. This includes information leaks that could be useful in potential memory corruption exploits, or exposure of sensitive user information that an attacker can exfiltrate. Bugs that would normally be rated at a higher severity level with unusual mitigating factors may be rated as medium severity.

0	0	3	0
Critical	**High**	**Medium**	**Low**

Differences since last assessment

New issues discovered		Previous issues remediated		Direction of travel
Critical	0	Critical	0	▲ 0
High	0	High	0	▲ 0
Medium	0	Medium	6	▲ -3
Low	0	Low	0	▲ 0

What we checked you for

Finds subdomains

Finds subdomains of a web server by querying Google's Certificate Transparency logs database

CSRF vulnerability

Detects Cross Site Request Forgeries (CSRF) vulnerabilities. It will try to detect them by checking each form if it contains an unpredictable token for each user. Without one an attacker may forge malicious requests

SSLv2 support

Determines whether the server supports obsolete and less secure SSLv2, and discovers which ciphers it supports

MySQL server with an empty password

Checks for MySQL server with an empty password for "root" or "anonymous"

SQL injection

Spiders an HTTP server looking for URLs containing queries vulnerable to an SQL injection attack. It also extracts forms from found websites and tries to identify fields that are vulnerable. The script spiders an HTTP server looking for URLs containing queries. It then proceeds to combine crafted SQL commands with susceptible URLs in order to obtain errors. The errors are analysed to see if the URL is vulnerable to attack

Test SSH weak passwords

Performs brute force TOP 100 password guessing against ssh server

XSS vulnerability

An indication of potential XSS vulnerability

Test Wordpress CMS/blog weak passwords

Performs brute force TOP 100 password Wordpress CMS

SSL certificate

Retrieves a server's SSL certificate. Prints the validity period and the commonName, organizationName, stateOrProvinceName, and countryName of the subject

Directory traversal vulnerability

Checks if a web server is vulnerable to directory traversal. The check uses several technique: - Generic directory traversal by requesting paths - Known specific traversals of several web servers - Query string traversal. This sends traversals as query string parameters to paths that look like they refer to a local file name

Detect insecure file upload forms

Detecting insecure file upload forms in web applications using various techniques like changing the Content-type header or creating valid image files containing the payload in the comment

Security headers

Checks for the HTTP response headers related to security given in OWASP Secure Headers Project and gives a brief description of the header and its configuration value. Checks for HSTS(HTTP Strict Transport Security), HPKP(HTTP Public Key Pins), X-Frame-Options, X-XSS-Protection, X-Content-Type-Options, Content-Security-Policy, X-Permitted-Cross-Domain-Policies, Set-Cookie, Expect-CT, Cache-Control, Pragma and Expires

SSL configurations

Check will warn about certain SSL misconfigurations such as MD5-signed certificates, low-quality ephemeral DH parameters, and the POODLE vulnerability. The end result is a list of all the ciphersuites and compressors that a server accepts. Each ciphersuite is shown with a letter grade (A through F) indicating the strength of the connection. The grade is based on the cryptographic strength of the key exchange and of the stream cipher. The message integrity (hash) algorithm choice is not a factor. The output line beginning with Least strength shows the strength of the weakest cipher offered. The scoring is based on the Qualys SSL Labs SSL Server Rating Guide, but does not take protocol support (TLS version) into account, which makes up 30% of the SSL Labs rating

FTP server allows anonymous

Checks if an FTP server allows anonymous logins. If anonymous is allowed, gets a directory listing of the root directory and highlights writeable files

Test MySQL weak passwords

Performs brute force TOP 100 password MySQL server

Test FTP weak passwords

Performs brute force TOP 100 password FTP server

Service Discovery & General Vulnerabilities Check

Discovers network assets, and then scans ports to identify key asset characteristics, such as operating system, device type, and services. Xsignal logs on to the asset and gathers information about the installed application inventory and required configuration, and raises vulnerabilities.

Enumerates web directories

Enumerates directories used by popular web applications and servers. Parses a fingerprint, building in advanced pattern matching as well as having the ability to identify specific versions of Web applications

Those are the checks that were made for this report. However, your service with us also includes:

Regular Checks

On average, more than 20 new vulnerabilities are discovered every day. A hacker may only need one of these to breach your systems. The Pro plan includes monthly checks for the latest weaknesses which may affect your systems, and ensures any recent changes haven't compromised your security.

Emerging Threats

The time between new vulnerabilities emerging and hackers exploiting them is now days, not weeks. For organisations who need a more mature approach to cyber security, our emerging threat scans detect critical threats to your systems without waiting for the next monthly check

Issue Summary

Impact	Issue details
medium	**The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.** Number of occurrences: 1
medium	**Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use** Number of occurrences: 1
medium	**The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation** Number of occurrences: 1

Issues

The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.

Description

https://nvd.nist.gov/vuln/detail/CVE-2017-15906

ampluart.ru : 23421	01 Aug 21 13:16 +0000
Cvss2: 5	Cvss2 Vector: AV:N/AC:L/Au:N/C:N/I:P/A:N
Cvss3: 5.3	Cvss3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
Severity	medium

The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation

Description

This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client).

https://nvd.nist.gov/vuln/detail/CVE-2020-14145

ampluart.ru : 23421	01 Aug 21 13:16 +0000
Cvss2: 4.3	Cvss2 Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N
Cvss3: 5.9	Cvss3 Vector: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
Severity	medium

Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use

Description

NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'

https://nvd.nist.gov/vuln/detail/CVE-2018-15919

ampluart.ru : 23421	01 Aug 21 13:16 +0000
Cvss2: 5	Cvss2 Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N
Cvss3: 5.3	Cvss3 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
Severity	medium

Scan info

Targets included in this scan

ampluart.ru

Scan timings

This scan ran from 01 Aug 21

Additional checks result

Finds subdomains

Description

Finds subdomains of a web server by querying Google's Certificate Transparency logs database.

SSL certificate

Description

Retrieves a server's SSL certificate. Prints the validity period and the commonName, organizationName, stateOrProvinceName, and countryName of the subject.

Port 443

Name certificate	Country name	Company name	From	To	
R3	US	Let's Encrypt	15 Mar 21 13:34	13 Jun 21 13:34	issue

Security headers

Description

Checks for the HTTP response headers related to security given in OWASP Secure Headers Project and gives a brief description of the header and its configuration value. Checks for HSTS(HTTP Strict Transport Security), HPKP(HTTP Public Key Pins), X-Frame-Options, X-XSS-Protection, X-Content-Type-Options, Content-Security-Policy, X-Permitted-Cross-Domain-Policies, Set-Cookie, Expect-CT, Cache-Control, Pragma and Expires.

Port 443

Header name	Header value	status
HSTS (HTTP Strict Transport Security)	HSTS not configured in HTTPS Server	success
X_Frame_Options	X_Frame_Options	issue
X_XSS_Protection	X_XSS_Protection	issue
X_Content_Type_Options	X_Content_Type_Options	issue
Content_Security_Policy	Content_Security_Policy	issue
X_Permitted_Cross_Domain_Policies	X_Permitted_Cross_Domain_Policies	issue
Cookie	Cookie	issue
Expect_CT	Expect_CT	issue
Cache_Control	Cache_Control	issue
Pragma	Pragma	issue
Expires	Expires	issue

Port 80

Header name	Header value	status
Strict_Transport_Security	Strict_Transport_Security	issue

Header name	Header value	status
X_Frame_Options	X_Frame_Options	issue
X_XSS_Protection	X_XSS_Protection	issue
X_Content_Type_Options	X_Content_Type_Options	issue
Content_Security_Policy	Content_Security_Policy	issue
X_Permitted_Cross_Domain_Policies	X_Permitted_Cross_Domain_Policies	issue
Cookie	Cookie	issue
Expect_CT	Expect_CT	issue
Cache-Control	Header: Cache-Control: no-store, no-cache, must-revalidate	success
Pragma	Header: Pragma: no-cache	success
Expires	Header: Expires: Thu, 19 Nov 1981 08:52:00 GMT	success

SSL configurations

Description

Check will warn about certain SSL misconfigurations such as MD5-signed certificates, low-quality ephemeral DH parameters, and the POODLE vulnerability. The end result is a list of all the ciphersuites and compressors that a server accepts. Each ciphersuite is shown with a letter grade (A through F) indicating the strength of the connection. The grade is based on the cryptographic strength of the key exchange and of the stream cipher. The message integrity (hash) algorithm choice is not a factor. The output line beginning with Least strength shows the strength of the weakest cipher offered. The scoring is based on the Qualys SSL Labs SSL Server Rating Guide, but does not take protocol support (TLS version) into account, which makes up 30% of the SSL Labs rating.

Directory traversal vulnerability

Description

Checks if a web server is vulnerable to directory traversal. The check uses several technique: - Generic directory traversal by requesting paths - Known specific traversals of several web servers - Query string traversal. This sends traversals as query string parameters to paths that look like they refer to a local file name.

SSLv2 support

Description

Determines whether the server supports obsolete and less secure SSLv2, and discovers which ciphers it supports.

XSS vulnerability

Description

An indication of potential XSS vulnerability.

Detect insecure file upload forms

Description

Detecting insecure file upload forms in web applications using various techniques like changing the Content-type header or creating valid image files containing the payload in the comment.

SQL injection

Description

Spiders an HTTP server looking for URLs containing queries vulnerable to an SQL injection attack. It also extracts forms from found websites and tries to identify fields that are vulnerable. The script spiders an HTTP server looking for URLs containing queries. It then proceeds to combine crafted SQL commands with susceptible URLs in order to obtain errors. The errors are analysed to see if the URL is vulnerable to attack.

Enumerates web directories

Description

Enumerates directories used by popular web applications and servers. Parses a fingerprint, building in advanced pattern matching as well as having the ability to identify specific versions of Web applications.

Web server catalogs were not found

There are no web server catalogs with known fingerprint

CSRF vulnerability

Description

Detects Cross Site Request Forgeries (CSRF) vulnerabilities. It will try to detect them by checking each form if it contains an unpredictable token for each user. Without one an attacker may forge malicious requests.

Test SSH weak passwords

Description

Performs brute force TOP 100 password guessing against ssh server.

Check successfully completed

No weak SSH passwords detected

MySQL server with an empty password

Description

Checks for MySQL server with an empty password for "root" or "anonymous".

Check successfully completed

No MySQL with anonymous access found

FTP server allows anonymous

Description

Checks if an FTP server allows anonymous logins. If anonymous is allowed, gets a directory listing of the root directory and highlights writeable files.

Check successfully completed

No FTP with anonymous access found

Test FTP weak passwords

Description

Performs brute force TOP 100 password FTP server.

Port 55555

Test MySQL weak passwords

Description

Performs brute force TOP 100 password MySQL server.

Check successfully completed

No weak MySQL passwords detected

Test Wordpress CMS/blog weak passwords

Description

Performs brute force TOP 100 password Wordpress CMS.

Check successfully completed

No weak passwords detected

xsignal.io

support@xsignal.io