

SAMPLE NETWORK INFRASTRUCTURE

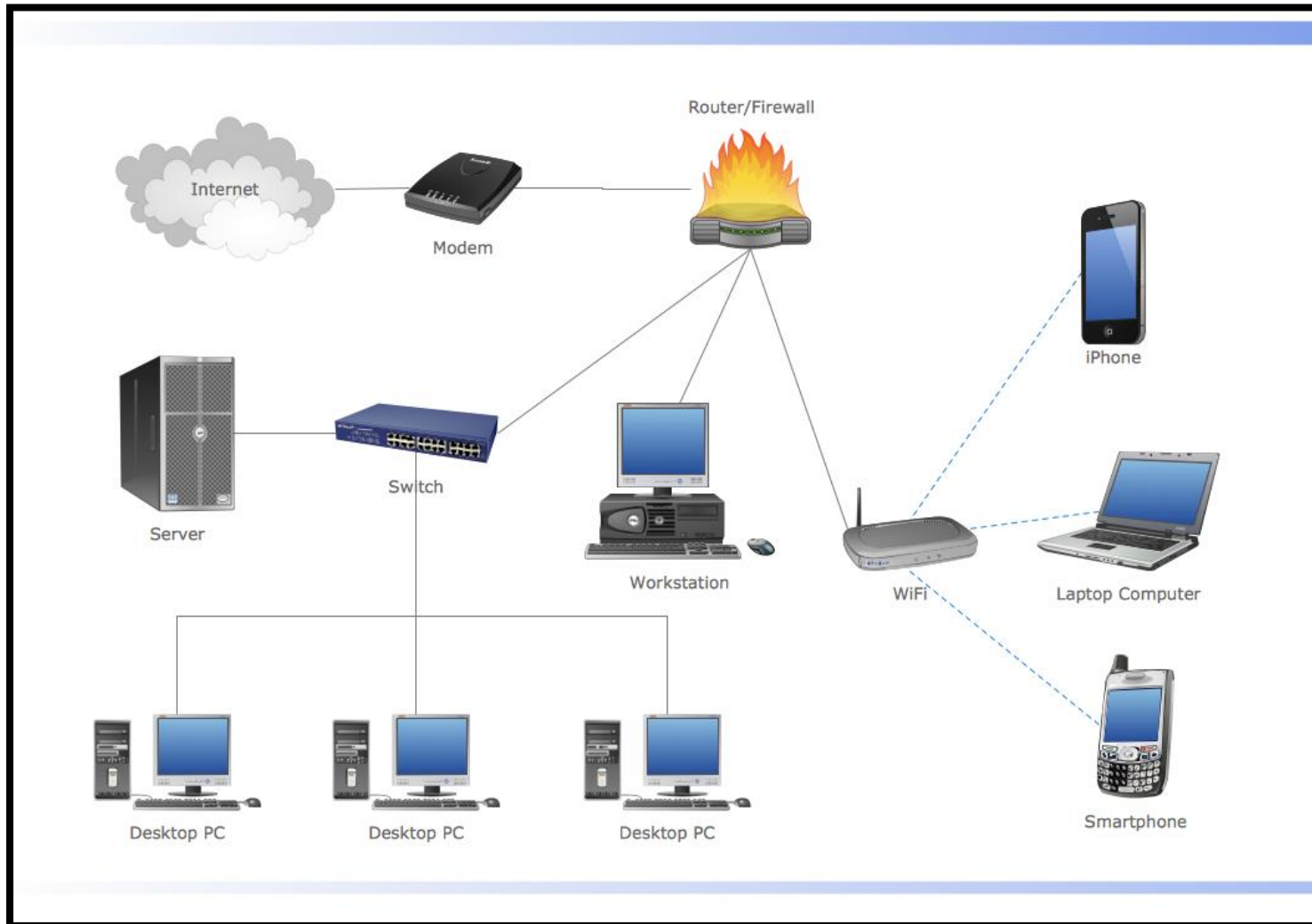


Photo credit : conceptdraw.com

Machine to scan against

Back [About Release](#) [Download](#) [Description](#) [File information](#) [Virtual Machine](#) [Networking](#) [Screenshot\(s\)](#) [Walkthrough\(s\)](#)

KIOPTRIX: LEVEL 1 (#1)

[About Release](#) [Back to the Top](#)

Name: Kioptrix: Level 1 (#1)
Date release: 17 Feb 2010
Author: Kioptrix
Series: Kioptrix
Web page: http://www.kioptrix.com/blog/?page_id=135

[Download](#) [Back to the Top](#)

Please remember that VulnHub is a free community resource so we are unable to check the machines that are provided to us. Before you download, please read our FAQs sections dealing with the dangers of running unknown VMs and our suggestions for "protecting yourself and your network. If you understand the risks, please download!

Kioptrix_Level_1.rar (Size: 186 MB)
Download: http://www.kioptrix.com/dlvm/Kioptrix_Level_1.rar
Download (Mirror): https://download.vulnhub.com/kioptrix/Kioptrix_Level_1.rar

Kioptrix is a downloadable VM image file on Vulnhub. It is a VM image challenge to get root access by any means possible. The goal of these is to learn the basic tools and techniques in vulnerability assessment and exploitation.

Scanning machine with Nessus vulnerability scanner



Nessus is a remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network.

Vulnerabilities discovered with Nessus Scanner

kioptrix

[Back to kioptrix](#)

ConfigureAudit TrailLaunchReportExport

Hosts1Vulnerabilities68Remediations2Notes17History1

FilterSearch Vulnerabilities68 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count		
<input type="checkbox"/>	CRITICAL	10.0	Apache httpd SEoL (<= 1.3.x)	Web Servers	1	🔄	✎
<input type="checkbox"/>	CRITICAL	9.8	9.0 Apache 2.4.x < 2.4.56 Multiple Vulnerabilities	Web Servers	1	🔄	✎
<input type="checkbox"/>	CRITICAL	9.8	6.7 Apache < 1.3.29 Multiple Modules Local Overflow	Web Servers	1	🔄	✎
<input type="checkbox"/>	CRITICAL	9.8	6.7 Apache < 2.4.49 Multiple Vulnerabilities	Web Servers	1	🔄	✎
<input type="checkbox"/>	CRITICAL	9.8	6.7 Apache 2.4.x < 2.4.53 Multiple Vulnerabilities	Web Servers	1	🔄	✎
<input type="checkbox"/>	CRITICAL	9.8	5.9 Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	Web Servers	1	🔄	✎
<input type="checkbox"/>	CRITICAL	9.1	5.2 Apache < 1.3.28 Multiple Vulnerabilities (DoS, ID)	Web Servers	1	🔄	✎
<input type="checkbox"/>	CRITICAL	9.0	9.2 Apache < 2.4.49 Multiple Vulnerabilities	Web Servers	1	🔄	✎
<input type="checkbox"/>	CRITICAL	9.0	6.5 Apache 2.4.x < 2.4.55 Multiple Vulnerabilities	Web Servers	1	🔄	✎
<input type="checkbox"/>	HIGH	9.3 *	5.9 OpenSSL < 0.9.8f Multiple Vulnerabilities	Web Servers	1	🔄	✎
<input type="checkbox"/>	HIGH	9.3 *	5.9 OpenSSL < 0.9.8s Multiple Vulnerabilities	Web Servers	1	🔄	✎

Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 4:52 PM
End: Today at 5:11 PM
Elapsed: 19 minutes

Vulnerabilities

- Critical
- High
- Medium
- Low
- Info

Apache httpd SEoL (<= 1.3.x)

The screenshot displays the Kioptrix vulnerability scanner interface for Plugin #171347. The top navigation bar includes buttons for 'Configure', 'Audit Trail', 'Launch', 'Report', and 'Export'. Below this, a tabbed interface shows 'Hosts' (1), 'Vulnerabilities' (68), 'Remediations' (2), 'Notes' (17), and 'History' (1). The main content area is titled 'CRITICAL Apache httpd SEoL (<= 1.3.x)'. It contains sections for 'Description', 'Solution', 'See Also', and 'Output'. The 'Description' section states that Apache httpd is less than or equal to 1.3.x and is no longer maintained. The 'Solution' section advises upgrading to a currently supported version. The 'See Also' section provides a link to the Apache announcement. The 'Output' section shows a list of hosts with their URLs, installed versions, security end of life dates, and time since security end of life. On the right side, there is a 'Plugin Details' section with fields for Severity, ID, Version, Type, Family, Published, and Modified. Below this is a 'Risk Information' section with fields for Risk Factor, CVSS v3.0 Base Score, CVSS v3.0 Vector, CVSS v2.0 Base Score, and CVSS v2.0 Vector. At the bottom right, there is a 'Vulnerability Information' section with fields for CPE and Unsupported by vendor.

kioptrix / Plugin #171347

Configure Audit Trail Launch Report Export

Hosts 1 Vulnerabilities 68 Remediations 2 Notes 17 History 1

CRITICAL Apache httpd SEoL (<= 1.3.x)

Description

According to its version, Apache httpd is less than or equal to 1.3.x. It is, therefore, no longer maintained by its vendor or provider.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it may contain security vulnerabilities.

Solution

Upgrade to a version of Apache httpd that is currently supported.

See Also

<http://archive.apache.org/dist/httpd/Announcement1.3.html>

Output

```
URL : http://192.168.43.180/
Installed version : 1.3.20
Security End of Life : February 2, 2010
Time since Security End of Life (Est.) : >= 14 years
```

To see debug logs, please visit individual host

Port Hosts

80 / tcp / www

Plugin Details

Severity: Critical
ID: 171347
Version: 1.4
Type: combined
Family: Web Servers
Published: February 10, 2023
Modified: November 2, 2023

Risk Information

Risk Factor: Critical
CVSS v3.0 Base Score 10.0
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

CPE: cpe:/a:apache:http_server
Unsupported by vendor: true

Mitigation for Apache httpd SEoL (<= 1.3.x):

Step 1: Identify Affected Systems

- Use vulnerability scanners or manual inspection to identify all systems running Apache httpd version 1.3.x.

Step 2: Verify Backup

- Before making any changes, ensure that you have a recent and verified backup of all critical data and configurations.

Step 3: Upgrade Apache httpd

- Download the latest version of Apache httpd (preferably version x.x.x or later) from the official Apache website.
- Follow the installation instructions provided with the Apache httpd package to install the new version.
- Ensure that all necessary dependencies are met and any custom configurations are migrated appropriately.

Step 4: Configuration Migration

- Review your existing Apache httpd configurations and ensure they are compatible with the new version.
- Make necessary adjustments to the configurations to ensure they work seamlessly with Apache httpd 2.4.x or later.
- Pay special attention to any deprecated or removed directives.

Step 5: Testing

- Test the new Apache httpd installation thoroughly in a non-production environment to ensure it functions correctly.
- Test various use cases, including serving web pages, handling different types of requests, and any custom configurations or modules.

Step 6: Deployment

- Once testing is successful, schedule a maintenance window to deploy the new Apache httpd version to production systems.
- Follow your organization's change management procedures for deploying changes to production systems.
- Monitor the deployment process closely to identify and address any issues promptly.

Step 7: Post-Deployment Testing

- After deployment, conduct thorough testing in the production environment to ensure that the new Apache httpd version is functioning as expected.
- Monitor system performance, error logs, and security logs for any abnormalities.
- Address any issues that arise during post-deployment testing promptly.

Estimated Timelines:

- The time required for mitigation depends on the complexity of your environment, the number of systems running Apache httpd 1.3.x, and the availability of resources.
- Planning and preparation: 1-2 weeks
- Testing and deployment: 1-2 weeks
- Post-deployment testing and monitoring: Ongoing

Required Resources:

- Personnel with expertise in Apache httpd administration and web server security.
- Access to non-production environments for testing.
- Backup systems and procedures.
- Change management processes for scheduling and deploying changes to production systems.
 - See also : <http://archive.apache.org/dist/httpd/Announcement1.3.html>

Changes to Network Configurations:

- In most cases, upgrading Apache httpd should not require significant changes to network configurations.
- However, ensure that firewalls, load balancers, and other network devices are configured to allow traffic to the new Apache httpd version on the appropriate ports.
- Update any network documentation to reflect the changes made during the upgrade process.

Apache 2.4.x < 2.4.56 Multiple Vulnerabilities

Vulnerabilities68

CRITICAL

Apache 2.4.x < 2.4.56 Multiple Vulnerabilities

<

>

Plugin Details✎

Description

The version of Apache httpd installed on the remote host is prior to 2.4.56. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.56 advisory.

- HTTP request splitting with mod_rewrite and mod_proxy: Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling attack. Configurations are affected when mod_proxy is enabled along with some form of RewriteRule or ProxyPassMatch in which a non-specific pattern matches some portion of the user-supplied request-target (URL) data and is then re-inserted into the proxied request-target using variable substitution. For example, something like: RewriteEngine on RewriteRule ^/here/(.*) http://example.com:8080/elsewhere?%1 http://example.com:8080/elsewhere ; [P] ProxyPassReverse /here/ http://example.com:8080/ http://example.com:8080/ Request splitting/smuggling could result in bypass of access controls in the proxy server, proxying unintended URLs to existing origin servers, and cache poisoning. Acknowledgements: finder: Lars Krapf of Adobe (CVE-2023-25690)

- Apache HTTP Server: mod_proxy_uwsgi HTTP response splitting: HTTP Response Smuggling vulnerability in Apache HTTP Server via mod_proxy_uwsgi. This issue affects Apache HTTP Server: from 2.4.30 through 2.4.55. Special characters in the origin response header can truncate/split the response forwarded to the client. Acknowledgements: finder: Dimas Fariski Setyawan Putra (nyxsorcerer) (CVE-2023-27522)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.56 or later.

Output

URL : http://192.168.43.180/
Installed version : 1.3.20
Fixed version : 2.4.56

To see debug logs, please visit individual host

Port ▲

Hosts

Severity: Critical

ID: 172186

Version: 1.6

Type: combined

Family: Web Servers

Published: March 7, 2023

Modified: October 21, 2023

VPR Key Drivers

Threat Recency: 120 to 365 days

Threat Intensity: Very Low

Exploit Code Maturity: PoC

Age of Vuln: 180 - 365 days

Product Coverage: Low

CVSSV3 Impact Score: 5.9

Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 9.0

Risk Factor: Critical

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:P/RL:O/RC:C

CVSS v3.0 Temporal Score: 8.8

CVSS v2.0 Base Score: 10.0

Mitigation Plan for Apache 2.4.x < 2.4.56:

1. Assessment of Current Environment:

- Identify all systems running Apache web server versions 2.4.x < 2.4.56.

- Determine the criticality of these systems and the potential impact of the vulnerability.
2. **Patch Deployment:**
 - Obtain the latest Apache x.x.xx release from the official Apache website or distribution repository.
 - Schedule a maintenance window for applying the patch to affected systems.
 - Notify stakeholders and coordinate with relevant teams for the patching process.
 3. **Remediation Steps:**
 - Stop the Apache web server service on each affected system.
 - Apply the patch by following the installation instructions provided with the update.
 - Restart the Apache service to ensure the changes take effect.
 4. **Testing:**
 - Conduct thorough testing to ensure that the patch installation does not cause any adverse effects on the web server's functionality.
 - Test critical web applications and services hosted on the Apache servers to verify their continued operation post-patch.
 5. **Timelines:**
 - Aim to complete the patch deployment within a defined maintenance window, considering the criticality of the vulnerability and the potential impact on operations.
 - Communicate the timeline to all stakeholders and adhere to any regulatory or compliance requirements.
 6. **Required Resources:**
 - Allocate sufficient resources, including personnel and hardware, to execute the patching process efficiently.
 - Coordinate with IT support teams to address any technical challenges that may arise during the patch deployment.
 7. **Network Configurations:**
 - Review and update firewall rules and access controls to ensure that the patched Apache servers are protected from unauthorized access.
 - Consider implementing additional security measures, such as intrusion detection/prevention systems, to enhance the overall security posture of the web server environment.

Apache 2.4.x < 2.4.55 Multiple Vulnerabilities

kioptrix / Plugin #170113

[Configure](#) [Audit Trail](#) [Launch](#) [Report](#) [Export](#)

Vulnerabilities 68

CRITICAL Apache 2.4.x < 2.4.55 Multiple Vulnerabilities

Description

The version of Apache httpd installed on the remote host is prior to 2.4.55. It is, therefore, affected by multiple vulnerabilities as referenced in the 2.4.55 advisory.

- A carefully crafted If: request header can cause a memory read, or write of a single zero byte, in a pool (heap) memory location beyond the header value sent. This could cause the process to crash. This issue affects Apache HTTP Server 2.4.54 and earlier. (CVE-2006-20001)
- 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 AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.54 and prior versions. (CVE-2022-36760)
- Prior to Apache HTTP Server 2.4.55, a malicious backend can cause the response headers to be truncated early, resulting in some headers being incorporated into the response body. If the later headers have any security purpose, they will not be interpreted by the client. (CVE-2022-37436)

Note that Nessus has not tested for these issues but has instead relied only on the application's self-reported version number.

Solution

Upgrade to Apache version 2.4.55 or later.

Output

```
URL           : http://192.168.43.180/
Installed version : 1.3.20
Fixed version  : 2.4.55
```

To see debug logs, please visit individual host

Port ▲	Hosts
--------	-------

Plugin Details

Severity: Critical

ID: 170113

Version: 1.5

Type: combined

Family: Web Servers

Published: January 18, 2023

Modified: March 10, 2023

VPR Key Drivers

Threat Recency: No recorded events

Threat Intensity: Very Low

Exploit Code Maturity: Unproven

Age of Vuln: 365 - 730 days

Product Coverage: Low

CVSSv3 Impact Score: 6.0

Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 6.5

Risk Factor: High

CVSS v3.0 Base Score 9.0

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/R:L/C:R/C:C

Mitigation Plan for Apache Apache 2.4.x < 2.4.55:

1. Step-by-Step Instructions for Remediation:

- Update Apache:** The primary step is to update Apache to version x.x.xx or higher, which contains the necessary patches to address the vulnerabilities.

- b. **Backup Configuration:** Before performing any updates, make sure to backup your existing Apache configuration files to avoid any loss of data or configuration settings.
- c. **Download Latest Version:** Download the latest version of Apache from the official Apache website or through your distribution's package manager.

2. **Estimated Timelines:**

The timeline for remediation will depend on the complexity of your Apache configuration and the availability of resources for updating and testing. However, the entire process, including updating, testing, and deploying the new version of Apache, can typically be completed within a few hours to a day.

3. **Required Resources or Changes to Network Configurations:**

- a. **Resource Allocation:** Allocate sufficient resources, including personnel and time, to perform the update and testing process.
- b. **Network Access:** Ensure that necessary network access is available to download the latest version of Apache and to test the updated installation.
- c. **Backup Resources:** Have backup resources available in case any issues arise during the update process, such as backups of configuration files and server data.

OpenSSL < 0.9.8f Multiple Vulnerabilities

The screenshot displays the Kioptrix Plugin #17760 interface. At the top, there are navigation buttons: Configure, Audit Trail, Launch, Report, and Export. Below the header, a tab labeled 'Vulnerabilities' shows 68 items. The selected vulnerability is 'OpenSSL < 0.9.8f Multiple Vulnerabilities', marked as 'HIGH'.

Description
According to its banner, the remote server is running a version of OpenSSL that is earlier than 0.9.8f. As such, it is affected by the following vulnerabilities:

- A local attacker could perform a side-channel attack against the Montgomery multiplication code and retrieve RSA private keys. Note that this has not been exploited outside a laboratory environment. (CVE-2007-3108)
- A remote attacker could execute arbitrary code by exploiting an off-by-one error in the DTLS implementation. (CVE-2007-4995)

Solution
Upgrade to OpenSSL 0.9.8f or later.

See Also
<http://www.nessus.org/u70ef9572c>
<http://www.nessus.org/u7cbc3fb3e>
<http://www.kb.cert.org/vuls/id/RGII-74KLP3>
<https://www.openssl.org/news/secadv/20071012.txt>

Output

```
Banner      : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
Reported version : 0.9.6b
Fixed version  : 0.9.8f
```

To see debug logs, please visit individual host

Port ▲	Hosts

Plugin Details

Severity:	High
ID:	17760
Version:	1.13
Type:	combined
Family:	Web Servers
Published:	January 4, 2012
Modified:	August 22, 2023

VPR Key Drivers

- Threat Recency: No recorded events
- Threat Intensity: Very Low
- Exploit Code Maturity: Unproven
- Age of Vuln: 730 days +
- Product Coverage: Low
- CVSSv3 Impact Score: 5.9
- Threat Sources: No recorded events

Risk Information

- Vulnerability Priority Rating (VPR): 5.9
- Risk Factor: High
- CVSS v2.0 Base Score: 9.3
- CVSS v2.0 Temporal Score: 6.9
- CVSS v2.0 Vector: CVSS2#AV:N/AC:M/Au:N/C:C
- /I:C/A:C

Mitigation Plan for OpenSSL < 0.9.8f

Step 1: Identify Affected Systems

- Use vulnerability scanners or manual inspection to identify systems running OpenSSL versions prior to 0.9.8f.

Step 2: Prioritize Systems

- Prioritize systems based on their criticality to the organization and the sensitivity of the data they handle.

Step 3: Patching or Upgrading OpenSSL

- For systems running OpenSSL versions < 0.9.8f, patch or upgrade OpenSSL to version 0.9.8f or higher.
- Obtain the latest version of OpenSSL from the official website or package repositories.
- Ensure compatibility with existing applications and dependencies before applying the update.
- Test the patch or upgrade in a controlled environment to verify its effectiveness and compatibility.

Estimated Timeline:

- Immediate: Begin the process of patching or upgrading OpenSSL on critical systems.
- Within 1-2 weeks: Complete patching or upgrading OpenSSL on all identified systems.

Step 4: Network Configuration Changes

- Update firewall rules or network access controls to restrict access to systems that have not been patched or upgraded.
- Implement additional network security measures to mitigate potential attacks targeting vulnerable systems.

Additional Resources

<http://www.nessus.org/u?0ef9572c>

<http://www.nessus.org/u?cbc3fb3e>

<http://www.kb.cert.org/vuls/id/RGII-74KLP3>

<https://www.openssl.org/news/secadv/20071012.txt>

OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption

kioptrix / Plugin #58799

[Back to Vulnerabilities](#)

ConfigureAudit TrailLaunchReportExport

Vulnerabilities68

HIGH

OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption

Description

According to its banner, the remote web server is running a version of OpenSSL earlier than 0.9.8w. As such, the OpenSSL library itself is reportedly affected by a memory corruption vulnerability via an integer truncation error in the function 'asn1_d2i_read_bio' when reading ASN.1 DER format data.

Applications using the 'BIO' or 'FILE' based functions (i.e., 'd2i_*_bio' or 'd2i_*_fp' functions) are affected by this issue. Also affected are 'S/MIME' or 'CMS' applications using 'SMIME_read_PKCS7' or 'SMIME_read_CMS' parsers. The OpenSSL command line utility is affected if used to handle untrusted DER formatted data.

Note that the SSL/TLS code of OpenSSL is not affected. Also not affected are applications using memory-based ASN.1 functions (e.g., 'd2i_X509', 'd2i_PKCS12', etc.) nor are applications using only PEM functions.

Note also that the original fix for CVE-2012-2110 in 0.9.8w was incomplete because the functions 'BUF_MEM_grow' and 'BUF_MEM_grow_clean', in file 'openssl/crypto/buffer/buffer.c', did not properly account for negative values of the argument 'len'.

Solution

Upgrade to OpenSSL 0.9.8w or later.

See Also

<https://www.openssl.org/news/secadv/20120419.txt>
<http://seclists.org/fulldisclosure/2012/Apr/210>
<https://www.openssl.org/news/secadv/20120424.txt>
<http://cvs.openssl.org/chgview?cn=22479>
<https://www.openssl.org/news/changelog.html>

Output

Banner : Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b

Reported version : 0.9.6b

Fixed version : 0.9.8w

To see debug logs, please visit individual host

Port ▲Hosts

< >

Plugin Details

Severity: High

ID: 58799

Version: 1.19

Type: combined

Family: Web Servers

Published: April 24, 2012

Modified: August 22, 2023

VPR Key Drivers

Threat Recency: No recorded events

Threat Intensity: Very Low

Exploit Code Maturity: PoC

Age of Vuln: 730 days +

Product Coverage: Low

CVSSv3 Impact Score: 5.9

Threat Sources: No recorded events

Risk Information

Vulnerability Priority Rating (VPR): 6.7

Risk Factor: High

CVSS v2.0 Base Score: 7.5

CVSS v2.0 Temporal Score: 5.9

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:P/A:P

CVSS v2.0 Temporal Vector: CVSS2#E:POC/RL:OF/RC:C

Vulnerability Information

Mitigation plan for OpenSSL < 0.9.8w ASN.1 asn1_d2i_read_bio Memory Corruption vulnerability

Patch OpenSSL:

- Obtain the latest version of OpenSSL (0.9.8w or higher) from the official website or your distribution's package manager.
- Apply the patch to all affected systems. This may involve downloading and compiling the source code or installing updated packages.

2. **Deploy the Patch:**

- Schedule a maintenance window to apply the patch.
- Notify all relevant stakeholders about the planned maintenance and potential downtime.
- Deploy the patch to all affected systems, including servers, workstations, and any other devices running OpenSSL.

3. **Testing:**

- Conduct thorough testing to ensure that the patch does not introduce any new issues or vulnerabilities.
- Test the functionality of applications and services that rely on OpenSSL to ensure they continue to work as expected.

4. **Monitor for Anomalies:**

- Implement monitoring solutions to detect any abnormal behavior or potential security incidents related to OpenSSL.
- Monitor system logs, network traffic, and other relevant indicators for signs of exploitation or compromise.

5. **Timeline:**

- The timeline for remediation will depend on the size and complexity of your environment, as well as any regulatory requirements or organizational policies.
- Aim to apply the patch as soon as possible after it becomes available to minimize the window of exposure to the vulnerability.

Additional Resources

<https://www.openssl.org/news/secadv/20120419.txt>

<http://seclists.org/fulldisclosure/2012/Apr/210>

<https://www.openssl.org/news/secadv/20120424.txt>

<http://cvs.openssl.org/chngview?cn=22479>

<https://www.openssl.org/news/changelog.html>

Browsable Web Directories

kioptrix / Plugin #40984
[Back to Vulnerabilities](#)

Configure Audit Trail Launch Report Export

Vulnerabilities 68

MEDIUM Browsable Web Directories

Description
Multiple Nessus plugins identified directories on the web server that are browsable.

Solution
Make sure that browsable directories do not leak confidential information or give access to sensitive resources. Additionally, use access restrictions or disable directory indexing for any that do.

See Also
<http://www.nessus.org/u?0a35179e>

Output

The following directories are browsable :

```
http://192.168.43.180/manual/  
http://192.168.43.180/manual/mod/  
http://192.168.43.180/manual/mod/mod_perl/
```

To see debug logs, please visit individual host

Port	Hosts
80 / tcp / www	

Plugin Details

Severity: Medium
ID: 40984
Version: 1.10
Type: remote
Family: CGI abuses
Published: September 15, 2009
Modified: January 19, 2021

Risk Information

Risk Factor: Medium
CVSS v3.0 Base Score 5.3
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CVSS v2.0 Base Score: 5.0
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N

Mitigation Plan for Browsable Web Directories:

1. Identify all publicly accessible web directories on your network: Use web scanning tools or automated vulnerability scanners to identify all directories that are browsable.
2. Disable directory browsing: Configure your web server (e.g., Apache, Nginx) to disable directory browsing. This can typically be done by modifying the server configuration files (e.g., httpd.conf for Apache) and setting the "Options" directive to disable "Indexes" or "AutoIndex".
3. Implement access controls: Restrict access to sensitive directories by using access control mechanisms such as password protection, IP whitelisting, or user authentication. This will help prevent unauthorized access to directory listings.

4. Remove unnecessary directories: Review the content of each directory and remove any unnecessary or unused directories. This will help reduce the attack surface and minimize the risk of exposure.
5. Regularly monitor for new directories: Implement regular scans or automated monitoring to detect any new directories that may become browsable inadvertently. This will help ensure ongoing compliance with security best practices.

Estimated Timelines:

- Identification of publicly accessible web directories: 1-2 days
- Disabling directory browsing and implementing access controls: 1-2 days
- Removal of unnecessary directories: Variable, depending on the number and complexity of directories
- Regular monitoring: Ongoing, with periodic checks scheduled at regular intervals (e.g., weekly, monthly)

Additional Recommendations

- Regularly update Apache HTTP Server and other software components to the latest stable versions to mitigate the risk of known vulnerabilities.
- Implement a robust firewall configuration to restrict access to Apache servers and minimize the attack surface.
- Employ intrusion detection and prevention systems (IDPS) to detect and block malicious activities targeting Apache servers.
- Stay informed about security advisories and patches released by the Apache Software Foundation and other relevant sources to proactively address emerging threats.
-
- Consider implementing intrusion detection and prevention systems to detect and block potential attacks targeting OpenSSL vulnerabilities.
- Educate system administrators and users about the importance of keeping software and systems up to date to mitigate security risks.
- Stay informed about security updates and patches released by OpenSSL and other software vendors to proactively address vulnerabilities.
- Educate website administrators and developers about the importance of securing web directories and following best practices for web server configuration.
- Consider implementing a web application firewall (WAF) to provide an additional layer of defense against malicious attacks targeting web directories.