IT22199508

Sri Lanka Institute of Information Technology

Bug Bounty Report 01

freshworks

IE2062 – Web Security

Submitted by:

IT22199508 – Athapaththu A.M.M.I.P

Date of submission

2024.05.04

Table of Contents

IT22199508

Vulnerability

1) Out-of-date Version (WordPress)

Date of Discovery: 20/04/2024

Date of Reporting: 21/04/2024

I am writing to inform you of a vulnerability that I have found in your website, https://www.freshworks.com . This vulnerability belongs to Vulnerable and Outdated components (A06-2021) of the OWASP top 10 vulnerabilities. This may lead to several risks of the website. You can see the detailed report of this vulnerability below.

- ## Description

The "Out-of-Date Version (OpenSSL) vulnerability" is a big security problem because it uses old and possibly not safe versions of the software called OpenSSL. OpenSSL is commonly used to safely send information over computer networks and is important for many online services and applications. Using an old version of OpenSSL can make your systems vulnerable to cyber threats like data breaches, attacks where someone secretly listens or changes your messages, and hackers being able to control your system from a distance. It is very important to fix this problem to keep digital messages and data safe and secure. Regularly updating OpenSSL to the latest secure versions, making sure to fix any problems, and checking for vulnerabilities are important steps to reduce the risk and protect sensitive information from being used by bad people.

- ## Impact Assessment

The following are some possible risks and effects for www.echobox.com that could arise from the vulnerability caused by using an outdated version of OpenSSL:

1. **Security Weakness:** Older versions of OpenSSL can have known flaws that are exploitable by hostile parties. This produces a security vulnerability that can allow unwanted access to private information or jeopardize the security of the website.

2. **Inaccurate Data:** Data breaches are more likely when OpenSSL is being used obsoletely. Cybercriminals may take use of well-known weaknesses in the OpenSSL version to obtain private user data, including payment information, login passwords, and personal information. Financial and legal repercussions may follow a data breach.

3. **Disagreement with Users:** Users anticipate a secure handling of their information. Users' trust and confidence in www.echobox.com's security procedures may be damaged if it is discovered that the website is employing obsolete and unsafe versions of OpenSSL. Users may become less engaged with the platform as a result and the website's reputation may suffer.

4. **Non-compliance with regulations:** Violating cybersecurity and data protection laws may result from using obsolete and insecure versions of OpenSSL. The reputation of the website could be harmed in addition to possible financial and legal repercussions.

The most recent secure version of OpenSSL should be quickly updated and patched by www.echobox.com to solve this vulnerability. To reduce these risks, it's crucial to routinely check for OpenSSL updates and implement security patches. The website will be able to improve security, preserve user confidence, guarantee regulatory compliance, and safeguard sensitive data by doing this. The precise consequences of this vulnerability are contingent upon the activities of possible aggressors and the vulnerabilities present in the obsolete version of OpenSSL.

- **Proof of Concept**

Request

```
GET /wp-includes/images/arrow-pointer-blue.png HTTP/1.1
Host: www.freshworks.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: fw_ue_ncta=[{%22source_click%22:%22AI%20that%20works%20for%20your%20business%22%2C%22source_pag
e%22:%22https://www.freshworks.com/%22%2C%22destination_url%22:%22javascript:void(0)%22}%2C{%22source_c
lick%22:%22AI%20that%20works%20for%20your%20business%22%2C%22source_page%22:%22https://www.freshworks.c
om/%22%2C%22destination_url%22:%22javascript:void(0)%22}]; fw_ue_cta=[{%22cta_click%22:%22Skip%20to%20m
ain%20content%22%2C%22cta_page%22:%22https://www.freshworks.com/%22%2C%22destination_url%22:%22#main-co
ntent%22}%2C{%22cta_click%22:%22Skip%20to%20main%20content%22%2C%22cta_page%22:%22https://www.freshwork
s.com/%22%2C%22destination_url%22:%22#main-content%22}%2C{%22cta_click%22:%22Skip%20to%20main%20conten
t%22%2C%22cta_page%22:%22https://www.freshworks.com/%22%2C%22destination_url%22:%22#main-content%22}%2C
{%22cta_click%22:%22Skip%20to%20main%20content%22%2C%22cta_page%22:%22https://www.freshworks.com/crm/sa
les/%22%2C%22destination_url%22:%22#main-content%22}%2C{%22cta_click%22:%22Start%20free%20trial%22%2C%2
2cta_page%22:%22https://www.freshworks.com/crm/sales/%22%2C%22destination_url%22:%22https://www.freshwo
rks.com/crm/signup/%22}%2C{%22cta_click%22:%22Skip%20to%20main%20content%22%2C%22cta_page%22:%22http
s://www.freshworks.com/crm/sales/%22%2C%22destination_url%22:%22#main-content%22}%2C{%22cta_click%22:%2
2Start%20free%20trial%22%2C%22cta_page%22:%22https://www.freshworks.com/crm/marketing/%22%2C%22destinat
ion_url%22:%22https://www.freshworks.com/crm/marketing/signup/%22}%2C{%22cta_click%22:%22Skip%20to%20ma
in%20content%22%2C%22cta_page%22:%22https://www.freshworks.com/crm/marketing/%22%2C%22destination_url%2
2:%22#main-content%22}%2C{%22cta_click%22:%22Explore%20e-commerce%20segments%22%2C%22cta_page%22:%22htt
ps://www.freshworks.com/crm/marketing/%22%2C%22destination_url%22:%22https://www.freshworks.com/crm/fea
tures/customer-segmentation/%22}]
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 2420.8281 Total Bytes Received : 2288 Body Length : 1569 Is Compressed : No

```
Binary response detected, response has not saved.
```

- ## Remediation

Please upgrade your installation of WordPress to the latest stable version

IT22199508

2) Missing X-Frame-Options Header

Date of Discovery: 20/04/2024

Date of Reporting: 21/04/2024

I am writing to inform you of a vulnerability that I have found in your website, https://www.freshworks.com . This vulnerability belongs to the Security Misconfigurations (A05)-2021 of the OWASP top 10 vulnerabilities. This may lead to several risks to the website. You can see the detailed report of this vulnerability below.

- ## Description

In online applications, the lack of an X-Frame-Options header poses a serious risk. This header is necessary to stop clickjacking attacks, in which malevolent parties try to insert a weak site inside an iframe on a different domain with the intention of inflicting damage. In the event that the X-Frame-Options header is incorrectly set, private data might be accessed or compromised. Web developers should always provide this header in the response of their application, indicating whether or not the page may be framed by other websites, in order to lessen the risk of this happening. This precaution is essential for maintaining the reliability and security of online material, thereby shielding consumers from potential security flaws and invasions of privacy.

- ## Impact Assessment

The Missing of the X-Frame-Options header on www.starbucks.com presents multiple vulnerabilities in the context of the OWASP category. If this security precaution isn't taken, bad actors could use Clickjacking and other attacks to undermine the integrity of the web application and possibly do a lot of damage. Should attackers be successful in using this vulnerability, the following situations might occur:

• Unauthorized Data Access: By deceiving visitors into inadvertently interacting with a website using Clickjacking, attackers can obtain sensitive user data, including financial information, login passwords, and personal information.

• Service Disruption: An attacker can interfere with the Starbucks website's operation by inserting a malicious frame into it, rendering it inaccessible to users for a short while or permanently. Financial losses as well as a bad user experience may result from this disruption.

• Malicious Use of Starbucks Domain: Phishing, denial-of-service, and malware distribution are just a few of the ways malicious actors may use the compromised Starbucks domain. This could hurt innocent customers in addition to damaging Starbucks' reputation.

It's crucial to remember that these are merely a few possible outcomes of taking advantage of this weakness. The precise strategies used by hostile actors and the weaknesses they take advantage of may determine the true effect of the attack. Starbucks must employ the X-Frame-Options header and other security steps to guard its web application and users in order to reduce these risks.

- **Proof of Concept**

Request

```
GET /freshservice/ HTTP/1.1
Host: www.freshworks.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
Cookie: fw_ue_ncta=[{%22source_click%22:%22AI%20that%20works%20for%20your%20business%22%2C%22source_pag
e%22:%22https://www.freshworks.com/%22%2C%22destination_url%22:%22javascript:void(0)%22}%2C{%22source_c
lick%22:%22AI%20that%20works%20for%20your%20business%22%2C%22source_page%22:%22https://www.freshworks.c
om/%22%2C%22destination_url%22:%22javascript:void(0)%22}]; fw_ue_cta=[{%22cta_click%22:%22Skip%20to%20m
ain%20content%22%2C%22cta_page%22:%22https://www.freshworks.com/%22%2C%22destination_url%22:%22#main-co
ntent%22}%2C{%22cta_click%22:%22Skip%20to%20main%20content%22%2C%22cta_page%22:%22https://www.freshwork
s.com/%22%2C%22destination_url%22:%22#main-content%22}%2C{%22cta_click%22:%22Skip%20to%20main%20conten
t%22%2C%22cta_page%22:%22https://www.freshworks.com/%22%2C%22destination_url%22:%22#main-content%22}]
Referer: https://www.freshworks.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.
77 Safari/537.36
X-Scanner: Netsparker
```

Response

Response Time (ms) : 3296.7527 Total Bytes Received : 375342 Body Length : 374358 Is Compressed : No

```
HTTP/1.1 200 OK
X-Cache: Hit from cloudfront
Age: 18603
Cache-Control: max-age=864000
ETag: "f2udapfn8k80oe"
Strict-Transport-Security: max-age=31536000; includeSubDomains
Transfer-Encoding: chunked
X-Amz-Cf-Id: dK7HuLWkwPa-iYnkaESrfjKxNjgphsLqQZsXEZkeKNn0LonEk1jkCw==
X-Content-Type-Options: nosniff
Connection: keep-alive
X-Frame-Options: allow-from https://www.freshworks.com
Vary: Accept-Encoding
X-Amz-Cf-Pop: BOM78-P2
Via: 1.1 eab832ea3e7350de6a54ba4f14b84024.cloudfront.net (CloudFront)
Content-Type: text/html; charset=utf-8
x-nextjs-cache: HIT
Content-Security-Policy: frame-ancestors 'self' *.freshworks.com *.freshdesk.com *.freshservice.com *.m
yfreshworks.com *.freshcaller.com *.freshteam.com *.freshchat.com *.freshping.io *.freshrelease.com *.f
reshstatus.io *.freshsuccess.com *.freshsuccess.io views.paperflite.com app.paperflite.com web.paperfli
te.com canvas.paperflite.com *.optimizely.com
Date: Thu, 09 May 2024 13:09:18 GMT
Content-Encoding:

<!DOCTYPE html><html lang="en"><head><meta charSet="utf-8"/><meta name="viewport" content="width=device
-width"/><link rel="preload" as="image" href="https://dam.freshworks.com/m/201271b18ba1bfc1/original/he
aderLogoDark.webp"/><link rel="preload" as="image" imageSrcSet="/_next/image/?url=%2Fimages%2FmobileLog
o.webp&amp;w=32&amp;q=75 1x, /_next/image/?url=%2Fimages%2FmobileLogo.webp&amp;w=64&amp;q=75 2x"/><titl
e>Freshservice - AI powered ITSM by Freshworks</title><meta name="google-site-verification" content="p1
kXiLh_RXdISzpdgWbzTnGp0pbeWIXKOYGHN98BTwc"/><meta name="description" content="Enterprise-level IT Servi
ce Ops, minus the complexity. Freshservice is easy to use, intelligent IT service management, powered b
y AI."/><meta name="application-name" content="Freshservice - AI powered ITSM by Freshworks"/><meta nam
e="robots" content="index, follow"/><link rel="canonical" href="https://www.freshworks.com/freshservic
e/"/><meta property="og:site_name" content="Freshworks"/><meta property="og:type" content=
…
```

- ## Remediation

Either use the DENYor SAMEORIGINheader value to support the majority of browsers. Additionally, you can define the frame ancestorsContent-Security-Policy directive.

IT22199508