



SLIIT

Discover Your Future

Sri Lanka Institute of Information Technology

Bug Bounty Report 09

zabbix

IE2062 – Web Security

Submitted by:

IT22199508 – Athapaththu A.M.M.I.P

Date of submission

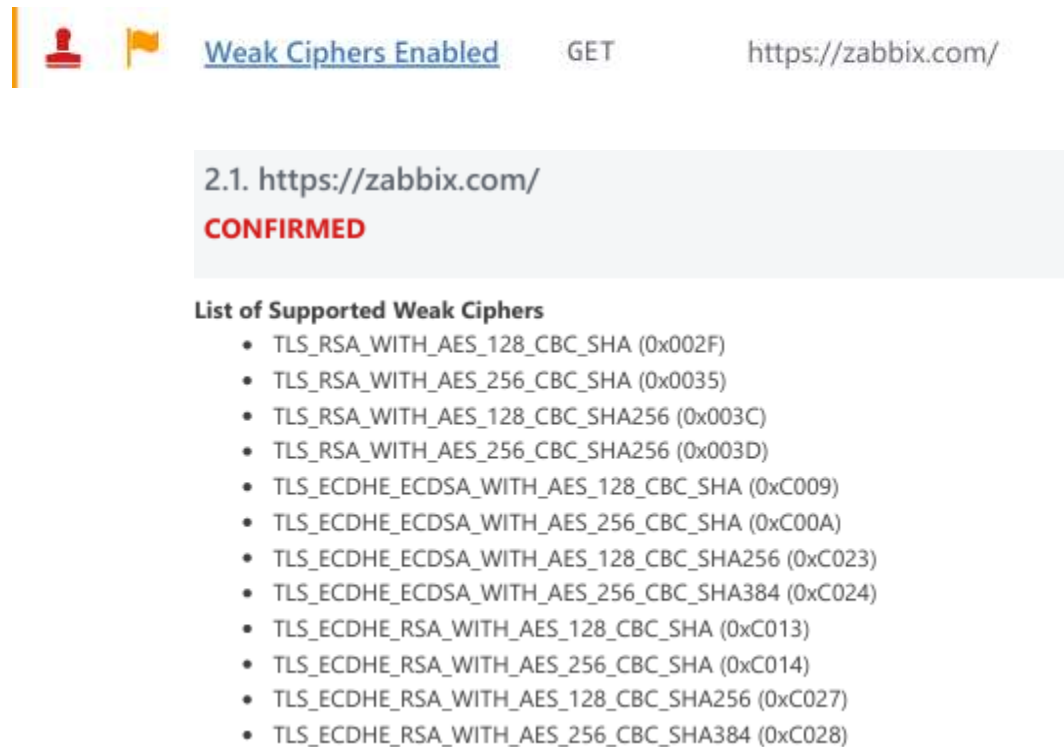
2024.05.04

Table of Contents

| | |
|---|----|
| Vulnerability | 3 |
| 1) Weak Ciphers Enabled | 3 |
| • Description | 4 |
| • Impact Assessment | 4 |
| • Request | 5 |
| • Response | 5 |
| • Steps to Reproduce | 5 |
| • Remediation | 6 |
| 2) HTTP Strict Transport Security (HSTS) Policy Not Enabled | 7 |
| • Description | 7 |
| • Impact Assessment | 8 |
| • Proof of Concept | 9 |
| • Remediation | 10 |

Vulnerability

1) Weak Ciphers Enabled



The screenshot shows a vulnerability report for 'Weak Ciphers Enabled' on the website https://zabbix.com/. The report is titled '2.1. https://zabbix.com/' and is marked as 'CONFIRMED'. Below the title, there is a list of supported weak ciphers.

2.1. https://zabbix.com/
CONFIRMED

List of Supported Weak Ciphers

- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xC009)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xC00A)
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xC023)
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xC024)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)

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, <http://zabbix.com/>. (A02) 2021: Cryptographic Failures shifts up one position to #2, previously known as Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often comes up to sensitive data exposure or system compromise. This may lead to several risks of the website. You can see the detailed report of this vulnerability below.

- **Description**

When activated, weak ciphers provide a serious risk to the safety of data and computer systems. These weak encryption methods give a gap that can be exploited by hostile actors since they are not complicated enough or strong enough to survive present cyberattacks. Attackers can intercept, decode and alter data by weakening the encryption used to secure sensitive information, jeopardizing the communication's secrecy and integrity. Given the importance of data security and privacy in today's linked society, this vulnerability is particularly serious.

- **Impact Assessment**

Under the OWASP category connected to poor Cipher Enabled vulnerabilities within the domain of **<http://zabbix.com/>**, various potential security threats have been found due to the usage of poor encryption protocols or ciphers. The impact of not addressing this vulnerability is considerable and includes the following potential,

consequences:

1. **Data Breaches:** The use of weak ciphers raises the risk of data breaches. If attackers successfully infiltrate the website, they may obtain access to a goldmine of sensitive user information, leading to potential data breaches and associated legal and financial penalties.
2. **Regulatory Non-Compliance:** Using weak ciphers may put Starbucks at variance with data protection rules and industry norms, potentially leading to legal and financial implications for non-compliance.
3. **Loss of User Trust:** Users expect their data to be handled securely. When weak ciphers are employed, it erodes trust in the website's security. This loss of trust can significantly damage the reputation and credibility of Starbucks and may lead to a reduction in customer confidence.
4. **Enhanced Attack Surface:** Weak ciphers may offer an enhanced attack surface for cybercriminals, making it easier for them to exploit weaknesses and gain unauthorized access to the website, its servers, and underlying systems.

It is vital to fix this Weak Cipher Enabled issue swiftly by adopting strong encryption methods and ciphers. Failure to do so not only expose users to potential security concerns but also damages Starbucks' reputation, legal compliance, and general corporate integrity. The repercussions of the vulnerability will depend on the actions taken by hostile actors and the level of the website's security flaws.

- **Request**

```
[NETSPARKER] SSL Connection
```

- **Response**

```
Response Time (ms) : 1    Total Bytes Received : 27    Body Length : 0    Is Compressed : No
```

```
[NETSPARKER] SSL Connection
```

- **Steps to Reproduce**

1. For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2. Lighttpd:

```
ssl.honor-cipher-order = "enable"  
ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

3. For Microsoft IIS, you should make some changes to the system registry. Incorrectly editing the registry may severely damage your system. Before making changes to the registry, you should back up any valued data on your computer.

- a. Click Start, click Run, type regedt32 or type regedit, and then click OK.

- b. In Registry Editor, locate the following registry key:

HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders

- c. Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56  
SCHANNEL\Ciphers\RC4 64/128  
SCHANNEL\Ciphers\RC4 40/128  
SCHANNEL\Ciphers\RC2 56/128  
SCHANNEL\Ciphers\RC2 40/128  
SCHANNEL\Ciphers\NULL  
SCHANNEL\Hashes\MD5
```

- **Remediation**

Configure your web server to disallow using weak ciphers.

2) HTTP Strict Transport Security (HSTS) Policy Not Enabled



1.1. https://zabbix.com/

| Error | Resolution |
|-------------------------------|--|
| preload directive not present | Submit domain for inclusion in browsers' HTTP Strict Transport Security (HSTS) preload list. |

Certainty



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://zabbix.com/>. This vulnerability belongs to Cryptographic Failures (A02) 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**

Web servers can declare that all interactions by web browsers and other user agents must take place over HTTPS connections and not unsecured HTTP connections by utilizing the HTTP Strict Transport Security (HSTS) web security policy mechanism. "Strict-Transport-Security" is an HTTP response header field that the server uses to transmit the HSTS Policy to the user agent. The HSTS Policy establishes a time frame for the user agent to exclusively employ secure methods of server access. An application that does not use HSTS may be vulnerable to downgrade, SSL-stripping, man-in-the middle, and cookie-hijacking attacks.

- **Impact Assessment**

The following are some possible outcomes and hazards associated with the vulnerability relating to the domain www.zabbix.com's lack of an activated HTTP Strict Transport Security (HSTS) policy:

1. **Security Weakness:** Downgrading attacks are possible in the absence of a HSTS policy, which gives hostile actors the ability to intercept or alter unprotected connections between users and the website. This may lead to security flaws that jeopardize user information.
2. **Man-in-the-Middle Attacks:** The website is vulnerable to man-in-the-middle (MitM) attacks in the absence of HSTS, which allow hackers to intercept and perhaps alter user-website communication. Data theft, illegal access, and other nefarious acts may result from this.
3. **Phishing and Data Theft:** By pretending to be www.echobox.com, cybercriminals may leverage this vulnerability to conduct phishing attacks and fool victims into disclosing sensitive information such login passwords, personal information, or bank account information. Financial losses and data theft may come from this.
4. **Loss of User Trust :** People anticipate private and safe internet communication. Users' confidence in the website's security may drop if HSTS isn't implemented, which may even lead them to stop visiting it altogether.
5. **Regulatory Non-Compliance:** Failure to implement HSTS may lead to violations of cybersecurity and data protection laws. Penalties and reputational harm are among the financial and legal repercussions that may result from this.

Turning on HSTS is essential to fixing this vulnerability. This security feature prevents downgrading attacks and improves overall security by guaranteeing that all communications with the website are encrypted and safe. Quick HSTS implementation can help the website comply with legal obligations, preserve user confidence, and protect user data. The precise consequences of this vulnerability are contingent upon the activities and potential attacks of malevolent individuals.

• Proof of Concept

Request

```
GET / HTTP/1.1
Host: www.zabbix.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
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) : 691.6828 Total Bytes Received : 226417 Body Length : 225231 Is Compressed : No

```
HTTP/1.1 200 OK
Report-To: [{"endpoints":[{"url":"https://a.nel.cloudflare.com/report/v4?s=pzLIQt1Hr5zrAmUdb5cVPAzvVGZLscR0JKP9P5OCaLTqNd%2BKFPS7v%2FA1G61Zsj1mgEFL%2BV0704ZeoBp%2FvQjCUBXclPaYH8pKoQQ8mQ5hsuXu0VjNPJxoViNvW0kk2bP"}], "group": "cf-nel", "max_age": 604800}]
CF-RAY: 88171012eaa792f5-CMB
access-control-allow-origin: *
cf-ipcountry: LK
set-cookie: zabbix_language=en; Domain=.zabbix.com; Path=/; Max-Age=86400; SameSite=Lax; HttpOnly; Secure
set-cookie: zbcfipc=LK; Domain=.zabbix.com; Path=/; Max-Age=86400; SameSite=Lax; Secure
strict-transport-security: max-age=31536000; includeSubDomains
Transfer-Encoding: chunked
Server: cloudflare
x-content-type-options: nosniff
x-xss-protection: 1; mode=block
Connection: keep-alive
referrer-policy: strict-origin
x-frame-options: SAMEORIGIN
vary: Accept-Encoding
NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
last-modified: Fri, 10 May 2024 00:08:20 GMT
Content-Type: text/html
cf-connecting-ip: 43.250.242.220
CF-Cache-Status: DYNAMIC
content-security-policy: frame-ancestors 'self' *.zabbix.com https://challenges.cloudflare.com
Date: Fri, 10 May 2024 04:07:31 GMT
Content-Encoding:

<!DOCTYPE html>
<html lang='en'>

<head>

<meta charset="utf-8">

<title>Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution</title>

<meta name="description" content="Zabbix is a mature and effortless enterprise-class open source monitoring solution for network monitoring and application monitoring of millions of metrics." >

<link rel="canonical" href="https://www.zabbix.com/index" />

<meta property="og:title" content="Zabbix :: The Enterprise-Class Open Source Network Monitoring Solution" />
<meta property="og:description" content="Zabbix is a mature and effortless enterprise-class open source
```

```
monitoring solution for network monitoring and application monitoring of millions of metrics." />
<meta property="og:type" content="website" />
<meta property="og:url" content="
...
```

- **Remediation**

- Ideally, after fixing the errors and warnings, you should consider adding your domain to the the HSTS preload list. This will ensure that browsers automatically connect your website by using HTTPS, actively preventing users from visiting your site using HTTP. Since this list is hardcoded in users' browsers, it will enable HSTS even before they visit your page for the first time, eliminating the need for Trust On First Use (TOFU) with its associated risks and disadvantages. Unless you fix the errors and warnings your website won't meet the conditions required to enter the browser's preload list:
- Browser vendors declared:
 - Serve a valid certificate
 - If you are listening on port 80, redirect all domains from HTTP to HTTPS on the same host. Serve all subdomains over HTTPS:
 - In particular, you must support HTTPS for the www subdomain if a DNS record for that subdomain exists
 - Serve an HSTS header on the base domain for HTTPS requests:
 - The max-age must be at least 31536000 seconds (1 year)
 - The includeSubDomains directive must be specified
 - The preload directive must be specified
 - If you are serving an additional redirect from your HTTPS site, that redirect must have the HSTS header (rather than the page it redirects to)

IT22199508