

**Dynamic Vulnerability Assessment**

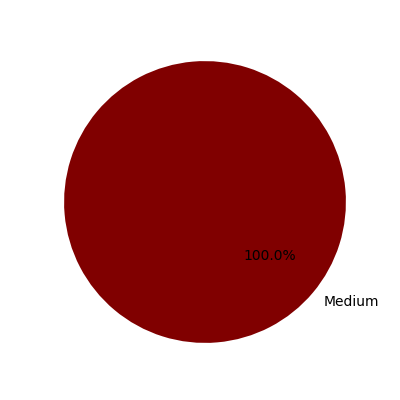
**srfgs**

**Requested by:** sdfh

## Version Information

|  |  |  |
| --- | --- | --- |
| Date | Application Version | Reviewer |
| 22-May-2025 | Initial Draft | sdh |
| 22-May-2025 | Peer Review |  |
| 22-May-2025 | Approved |  |

**Vulnerability Severity Distribution**



## Summary Table

|  |  |  |  |
| --- | --- | --- | --- |
| Sl. No. | Security Observation | Risk Rating | Page No. |
| **Medium Severity** | | | |
| 1 | Insecure Transport: Weak SSL Ciphers | Medium | 4 |

## URLs and Scope

URLs: sdfh

Scope: sdfh

## Vulnerability Details

### 1. Insecure Transport: Weak SSL Ciphers

**Severity: Medium**

CVSS Score: 6.7

CVSS Vector: CVSS:3.1/AV:A/AC:H/PR:L/UI:N/S:U/C:L/I:H/A:H

#### Description

Improper The Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols provide a  
mechanism to help protect authenticity, confidentiality and integrity of the data transmitted between a  
client and web server. The strength of this protection mechanism is determined by the authentication,  
encryption and hashing algorithms. These are collectively known as a cipher suite chosen for the  
transmission of sensitive information over the TLS/SSL channel. Most web servers support a range of such  
cipher suites of varying strengths. Using a weak cipher or an encryption key of insufficient length, for  
example, could enable an attacker to defeat the protection mechanism and steal or modify sensitive  
information. If misconfigured, a web server could be manipulated into choosing weak cipher suites. A  
weak encryption scheme can be subjected to brute force attacks that have a reasonable chance of  
succeeding using current methods and resources. An attacker could possibly execute a man in the middle  
attack which would allow them to intercept, monitor and tamper with sensitive data. Each weak cipher  
was enumerated by establishing an SSL connection with the target host and specifying the cipher to test  
in the Client Hello message of the SSL handshake.

#### Evidence

#### Recommendation

It is recommended not to use RC4, CBC,SHA, SHA1, MD5 etc ciphers

#### Reference

https://www.acunetix.com/blog/articles/tls-ssl-cipher-hardening/  
http://zero.webappsecurity.com