

TECHNICAL SECURITY REPORT

Detailed Vulnerability Analysis

Target: <https://www.sbsinformatique.com> | Generated: 2025-12-18T13:31:52.242Z

VULNERABILITY DETAILS

MEDIUM: SSL/TLS Configuration Weakness

Server supports weak cipher suites that could be exploited.

INFO: Information Disclosure via Server Banner

Server reveals detailed version information in response headers.

EXPLOITATION EVIDENCE

- Not Exploited: SSL/TLS Downgrade Attack
- Not Exploited: Generic Exploit Attempt

REMEDIATION CODE SNIPPETS

SSL/TLS Configuration Weakness

Language: nginx | Effort: 1-2 hours

```
ssl_protocols TLSv1.2 TLSv1.3;
ssl_ciphers ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256;
ssl_prefer_server_ciphers off;
```

Implementation: Update SSL/TLS configuration to use only modern protocols and cipher suites.

Information Disclosure via Server Banner

Language: text | Effort: 2-4 hours

```
# Remediation steps for: Information Disclosure via Server Banner
1. Review the vulnerability details
2. Apply vendor patches if available
3. Implement compensating controls
4. Verify fix through re-testing
```

Implementation: Follow vendor recommendations and security best practices for this vulnerability type.