Security Audit (Penetration Testing) Interim Report - STRUMIS Limited

2023 Q2 - External Use

Completed By: Joshua Mordecai (IT Manager – STRUMIS Ltd) & Intruder.io (Automated Attack Surface Monitor - External)

Completed On: 17th May 2023 with amendments on 26th May 2023

Report Type: Interim Manual & Automated Testing

Audit validity: 90 day(s)

Contents

Executive Summary:

The purpose of this penetration test was to assess the security posture of STRUMIS Ltd's internal and external systems and the STRUMIS application (including STRUMIS web services) and applications that host IP and identify vulnerabilities that could be exploited by potential attackers. The test was conducted by STRUMIS Ltd between 7th April 2023 and 26th May 2023. The primary objective was to evaluate the effectiveness of the existing security controls and recommend appropriate remediation measures on an interim basis for the purpose of reporting effective security controls. This report has been limited to the following scope for this objective.

Scope:

The scope of the penetration test included the following systems and networks:

STRUMIS Limited Internal Network, User Devices, Wireless AP's.
STRUMIS LLC Internal Network, User Devices, Wireless AP's.

Hosted Infrastructure – Microsoft Azure VM's and Services.
Hosted Services – Communication Platforms, Data storage.

STRUMIS Limited External Network & Load Balancing services & Watchguard Firewall Services (DDOS Protection).
STRUMIS LLC External Network & Watchguard Firewall Services.

STRUMIS Limited External VPN Services.

STRUMIS Product Web Service (Release Candidate).
STRUMIS Product SQL Configuration and Installation.
STRUMIS Product Client Configuration and Installation.

STRUMIS Product Mobility Application (Release Candidate).

Digital Social Engineering – M365 Compliance Insider Risk Management.

The test focused on identifying vulnerabilities and assessing the overall security of the systems from external and internal perspectives. The scope also encompassed digital social engineering attempts to evaluate the organization's security awareness and employee response to phishing and other targeted attacks.

Methodology:

The penetration test followed a systematic approach based on industry-standard methodologies, including the following phases:

a) Reconnaissance: Gathered information about the target systems and networks using both passive and active techniques.

Tools used – Nmap, Recon-ng, OSINT Framework Toolkit.

b) Scanning and Enumeration: Conducted port scanning and service enumeration to identify open ports, running services, and potential vulnerabilities.

Tools used – Watchguard Port Scanner, Intruder.io Surface Scanner.

c) Vulnerability Assessment: Performed a comprehensive vulnerability assessment of the target systems and networks using both automated tools and manual techniques.

d) Software & Source Code Vulnerability Assessment: Performed continual source code analysis for injection attempts, SQL injection flaws, known dependency vulnerabilities and zero-day vulnerabilities.

Tools user – OWASP Toolkit, Redgate Toolkit, Internal Code Review.

e) Exploitation: Attempted to exploit identified vulnerabilities to gain unauthorized access to the target systems.

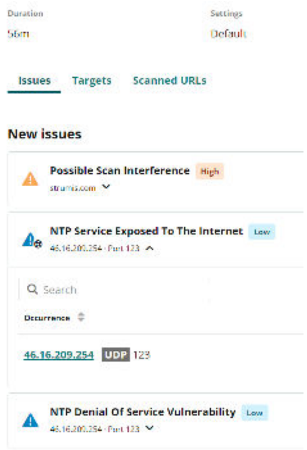
f) Post-Exploitation: Conducted further enumeration, privilege escalation, and lateral movement within the network to assess the extent of damage an attacker could cause.

g) Reporting: Documented all findings, including vulnerabilities discovered, their potential impact, and recommendations for remediation. The full report is outside the scope of this document for the purposes of reporting steps taken to demonstrate security controls. A summary of findings are documented in the next section.

Findings:

a) External Network Vulnerabilities 2023 Q2:

Identified open ports and services, including NTP Service availability external to the STRUMIS Limited network -



Duration
56m

Settings
Default

Issues Targets Scanned URLs

New issues

Possible Scan Interference High
strumis.com

NTP Service Exposed To The Internet Low
46.16.200.254 · Port 123

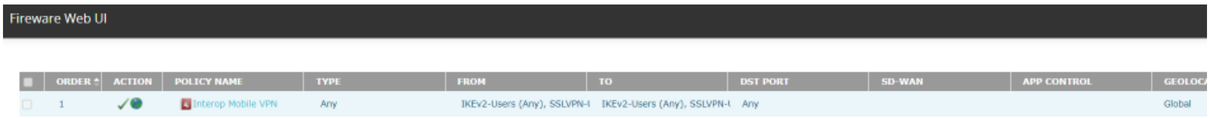
Search

Occurrence

46.16.209.254 UDP 123

NTP Denial Of Service Vulnerability Low
46.16.200.254 · Port 123

Discovered misconfigurations in firewall configuration, due to mobile VPN interop between internal and external STRUMIS Limited network, this was replicated on the STRUMIS LLC network. -



Fireware Web UI

□	ORDER	ACTION	POLICY NAME	TYPE	FROM	TO	DST PORT	SD-WAN	APP CONTROL	GEOLOCA
□	1	✓●	Interop Mobile VPN	Any	IKEv2-Users (Any), SSLVPN-I	IKEv2-Users (Any), SSLVPN-I	Any			Global

No vulnerable web applications to hosted or external networks were detected during this penetration test.

b) Internal Network Vulnerabilities:

Identified missing security patches and outdated software versions specific to some STRUMIS Networked devices, specifically remote end-user devices.

Discovered weak or easily guessable user passwords in the STRUMIS network applications that do not incorporate SSO (Microsoft AAD used as the primary authentication method)

c) Social Engineering:

Actor was unable to execute phishing attacks targeting Accounts & Sales staff, all incidents were reported to it.support@strumis.com or IT Management directly within 2-3hours or automatically quarantined by M365 security policies.

Found poor employee lack of adherence to security policies along with the use of weak passwords where possible.

d) STRUMIS Product Testing

Identified no malicious changes to signed DLL’s generated for the release candidate of the STRUMIS product and it’s dependencies.

Use of the http protocol and port 80 for the STRUMIS webservice as default was identified as a potential vulnerability.

Risk Assessment:

Based on the findings, a risk assessment will be conducted this quarter to determine the potential impact and likelihood of exploitation for each identified vulnerability. The risk assessment will consider the following factors:

Potential impact on the organization's confidentiality, integrity, and availability.

The ease of exploitation and likelihood of an attacker successfully leveraging the vulnerability.

Existing compensating controls and mitigating factors.

Recommendations and remediation:

To address the identified vulnerabilities and improve the overall security posture, the following recommendations are provided:

a) External Network:

NTP DDOS vulnerability – Watchguard Firewall policies have been updated to mitigate this vulnerability.

VPN specific vulnerability - Watchguard Firewall policies have been updated to mitigate this vulnerability.

Conduct regular external vulnerability assessments and penetration tests.

b) Internal Network:

Apply patches and updates to all network devices, Microsoft SCCM and ManageEngine Endpoint Central have been amended to commit patches at earlier intervals.

Enforce strong password policies and implement multi-factor authentication.

c) Social Engineering:

Implement further email filtering and detection mechanisms to identify and block phishing attempts that were received by STRUMIS staff and were not automatically quarantined by usual Microsoft 365 security policies.

Establish incident response procedures to handle security incidents.

Conclusion:

The interim penetration test revealed vulnerabilities and weaknesses in the security controls of STRUMIS Limited internal and external networks. These vulnerabilities were investigated and remedied, and a follow-up risk assessment performed.

The nature of these vulnerabilities was classified as “LOW RISK”.

Confidentiality:

This report contains sensitive information about the vulnerabilities discovered during the penetration test. As an interim test it should be treated as confidential and shared only with authorized individuals.

If you have any questions or require further clarification on any aspect of this report, please feel free to contact STRUMIS Limited at it.support@strumis.com

Sincerely,

Joshua Thomas Mordecai

IT Manager

STRUMIS Limited