FiberPatrol® FP1150 and Network Manager Penetration Testing Results

Senstar contracted an established cybersecurity consultancy to perform cyber penetration testing on a combined FiberPatrol FP1150 and Network Manager system. The objectives of the testing were as follows:

- Test the system for vulnerabilities that would enable an attacker to gain access to or control of the machine from over the network
- Test the system for vulnerabilities that would allow an attacker to take control of the physical security monitoring aspect of the system and either disable the detection capabilities of the system or create decoy alarms.

A redacted version of the pen testing report provided by the cybersecurity consultant is attached as Appendix A. The redaction conforms to the confidentiality terms of the cybersecurity consultant. The pen testing report highlights one issue considered to be high-risk, that being the lack of an authenticated and encrypted communications with external systems. Since the time the pen testing report was prepared, this issue has been addressed with the addition of TLS 1.2 support.

Other potential risks identified in the report have also since been addressed, namely patch management and the lack of running an anti-virus program.

SUMMARY

The combination of Senstar's FiberPatrol FP1150 fiber optic intrusion detection sensor and the Network Manager software provides a high level of cybersecurity and can be safely connected to security networks.

Contact Senstar for further information on the FiberPatrol FP1150, Network Manager software, and other Senstar products.

Version: R1 09/20

[redacted]

FiberPatrol Network Assessment

Senstar

May 13, 2019 – Version 1.1

Prepared for

[redacted]

[redacted]

[redacted]

Executive Summary

Synopsis

During the Spring of 2019, Senstar engaged [redacted] to conduct a network security assessment of the FiberPatrol-PR application that runs within the FiberPatrol unit. The FiberPatrol unit provides a fiber optic intrusion detection system. The application is used as a perimeter monitoring system that provides a detailed alarm report if the perimeter is crossed. For this engagement, [redacted] performed testing with a FiberPatrol unit Senstar shipped to [redacted] office in [redacted] Network penetration testing was synthetic and based on a simulated network environment configured by [redacted]

Scope

[redacted] evaluation included:

- **FiberPatrol-PR** Application that provides alarm monitoring reports and detailed feeds of intrusion.

Testing was performed in a simulated network to perform a network penetration test against the FiberPatrol Unit. To adequately assess the security standing of the FiberPatrol(-PR), this environment did not assume any firewalling or network security configurations. The testing laptop was connected to the FiberPatrol Unit via cross over cable, this allowed for analysis and testing of network exposure.

Key Findings

The assessment identified two issues:

- **Application Communication is Unauthenticated and Unencrypted:** [redacted] identified a lack of authenticity, integrity, and encryption on the FiberPatrol alarm report feeds, which would enable a sufficiently positioned attacker on the network to modify and deceive reliant security systems (i.e. provide false alarms).
- **Automatic Updates Disabled:** Future updates are not automatically delivered to the FiberPatrol unit, thereby preventing protection from future vulnerabilities.

Limitations

[redacted] was unable to evaluate all components within the application platform.

- The test device was setup, troubleshooted, and received on the second day of testing.
- Components such as cabling had to be sourced separately.
- A proper and thorough build review of the environment was not fully evaluated within the time of the engagement.
- The limited time frame of the engagement enabled only a basic network and build assessment of the FiberPatrol unit.

Strategic Recommendations

- Consider implementing encapsulation of services within TLS for clients to ensure authenticity and integrity of the traffic.
- Senstar should further evaluate mitigations, defense in depth strategies, and security guides for end users configuring their FiberPatrol units.
- In the unit's current state, there is a list of risks associated with deploying as-is. These risks should be adequately communicated with customers who use the FiberPatrol unit so that they may attempt to secure the system as it exists in production deployments. A list of such potential risks is included in Potential Accepted Risks on the following page.
- Senstar should perform a comprehensive assessment of the attack surface, including an assessment of listening services (ex: license server, web server, netbios, rpc) , a host build review, and a thick client review.

Potential Accepted Risks

- The TCP-based service that external systems use to communicate to the FiberPatrol system — to the Network Manager software in particular — is not strictly authenticated and will successfully respond to any network nodes included in the Network Manager IP whitelist.
  - ***Evaluation:*** Multiple ports were allowing connections without authentication.
- Communications between the Network Manager software running on the FiberPatrol unit and external systems are not encrypted.
  - ***Evaluation:*** Communications between the FiberPatrol unit and external systems are not encrypted.
- The system was missing latest Windows patches.
  - ***Evaluation:*** The environment was recently updated, however automatic updates were not enabled.
- The system was not running an anti-virus program or a complete application whitelisting solution.
  - ***Evaluation:*** [redacted] observed a limited set of restrictions on allowed applications implemented via Local Security Policy.
- The system runs several unnecessary services that may increase its attack surface.
  - ***Evaluation:*** Although some unnecessary services did appear to be disabled, several other running services were identified that were unlikely to be necessary.
- Several services and processes run with excessively high privileges.
  - ***Note:*** FiberPatrol application runs with System privileges. The Network Manager software also runs with Administrator level privileges. This is required by design.
- The FiberPatrol system is configured with auto-login enabled.
  - ***Note:*** After some discussion, this appears to be a design necessary so that the system starts up automatically after bootup.
- The system uses weak default passwords and password policies.
  - ***Evaluation:*** Although the FiberPatrol application has a default password of [redacted], the password is set by the end user. However, the FiberPatrol application does not enforce password complexity rules.

Dashboard

Target Metadata

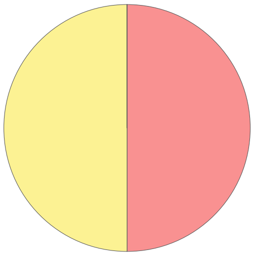
Name	FiberPatrol
Type	Simulated Internal
Platforms	Windows
Environment	Local Instance

Engagement Data

Type	Network Penetration Test
Method	Black-box
Dates	2019-04-29 to 2019-05-02
Consultants	1
Level of effort	4 person-days

Finding Breakdown

Critical Risk issues	0
High Risk issues	1
Medium Risk issues	0
Low Risk issues	1
Informational issues	0
Total issues	**2**



Category Breakdown

Data Exposure	1	🟥
Patching	1	🟨

Key

Critical 🟥 High 🟥 Medium 🟧 Low 🟨 Informational ⬜

Table of Findings

For each finding, [redacted] uses a composite risk score that takes into account the severity of the risk, application's exposure and user population, technical difficulty of exploitation, and other factors. For an explanation of [redacted] risk rating and finding categorization, see Appendix A on page 8.

Title	ID	Risk
Application Communication is Un-Authenticated & Un-Encrypted	001	High
Automatic Updates Disabled	002	Low

Finding Details

Finding **Application Communication is Un-Authenticated & Un-Encrypted**

Risk High Impact: High, Exploitability: Medium

Identifier [redacted]

Category Data Exposure

Location Port 4122/TCP

Impact Attackers on the network can intercept and modify traffic, such as Alarm Reports to provide false intrusion information.

Description The FiberPatrol application listens on TCP port 4122, and allows any client on the network to connect and receive XML feeds. These XML feeds are transmitted over the network without authentication or encryption. The contents of the XML elements include values consisting of alarm time, system time, coordinates, etc. A sufficiently positioned attacker on the network who can intercept the raw traffic — e.g. with ARP spoofing — could trivially modify these values and deceive security monitoring systems that rely on these XML feeds to detect an intrusion.

Example connection attempt:

```
nc -vv 192.168.0.2 4122
```

Example truncated Alarm Report response containing coordinates, alarm time, duration, location etc.

```
<?xml version="1.0"?>
<AlarmReport>
...
<SystemTime>3639574016.43</SystemTime>
<SystemStatus>65</SystemStatus>
<CutLocation1>41</CutLocation1>
<CutLocation2>63</CutLocation2>
...
<AlarmTime>3639573985.32</AlarmTime>
...
<Duration>30.77</Duration>
<Position>-1000</Position>
...
<Coordinates>40.146753,-74.848733,0.00</Coordinates>
...
<EventTime>3639573985.32</EventTime>
...
</AlarmReport>
```

Recommendation Where possible, un-encrypted protocols should be replaced with encrypted alternatives based on authenticated encryption. Additionally, consider encapsulating sensitive information within TLS, thereby allowing encrypted and authenticated connections to receive alarm reports XML feeds.

Finding: Automatic Updates Disabled

Risk Low Impact: Low, Exploitability: Low

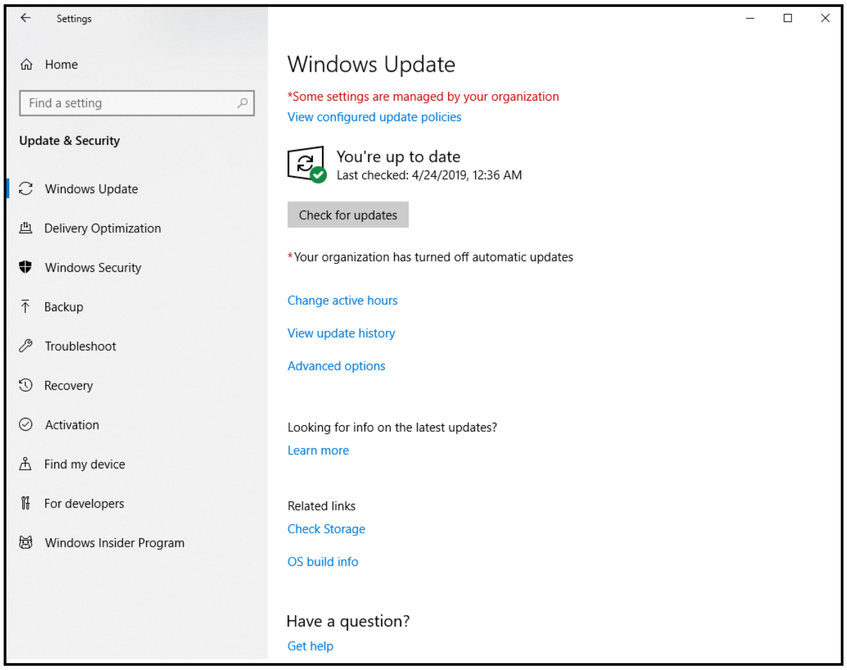
Identifier [redacted]

Category Patching

Location FiberPatrol Windows Environment

Impact Attackers can potentially leverage recently publicly-disclosed vulnerabilities and public exploit code to attack unpatched systems.

Description During this assessment, [redacted] identified that while the system under test was very recently updated (24 April 2019), it was configured such that automatic updates were disabled. As this system represents a production deployment, this would imply that production systems may not be adequately updated after setup. This introduces significant risk as the timely application of future patches are critical to ensuring that known vulnerabilities are addressed appropriately to prevent such systems from being compromised through otherwise patched vulnerabilities.



Windows Update

*Some settings are managed by your organization

View configured update policies

You're up to date

Last checked: 4/24/2019, 12:36 AM

*Your organization has turned off automatic updates

Looking for info on the latest updates?

Have a question?

Figure 1: Automatic Updates Disabled

Recommendation Windows security patches should be applied in a timely manner and all Windows servers should be included in an active patch management program. Failure to do so can lead to compromise of both the individual server and any associated domain. Furthermore, Senstar should design, implement, and test a patch management solution and associated patch management policy to ensure that systems are adequately protected from vulnerabilities.

Windows Update can be used for standalone or small deployments, and SUS/WSUS for enterprise environments. Additionally, a number of commercial solutions also exist.

Appendix A: Finding Field Definitions

The following sections describe the risk rating and category assigned to issues [redacted] identified.

Risk Scale

[redacted] uses a composite risk score that takes into account the severity of the risk, application's exposure and user population, technical difficulty of exploitation, and other factors. The risk rating is [redacted] recommended prioritization for addressing findings. Every organization has a different risk sensitivity, so to some extent these recommendations are more relative than absolute guidelines.

Overall Risk

Overall risk reflects [redacted] estimation of the risk that a finding poses to the target system or systems. It takes into account the impact of the finding, the difficulty of exploitation, and any other relevant factors.

Critical Implies an immediate, easily accessible threat of total compromise.

High Implies an immediate threat of system compromise, or an easily accessible threat of large-scale breach.

Medium A difficult to exploit threat of large-scale breach, or easy compromise of a small portion of the application.

Low Implies a relatively minor threat to the application.

Informational No immediate threat to the application. May provide suggestions for application improvement, functional issues with the application, or conditions that could later lead to an exploitable finding.

Impact

Impact reflects the effects that successful exploitation upon the target system or systems. It takes into account potential losses of confidentiality, integrity and availability, as well as potential reputational losses.

High Attackers can read or modify all data in a system, execute arbitrary code on the system, or escalate their privileges to superuser level.

Medium Attackers can read or modify some unauthorized data on a system, deny access to that system, or gain significant internal technical information.

Low Attackers can gain small amounts of unauthorized information or slightly degrade system performance. May have a negative public perception of security.

Exploitability

Exploitability reflects the ease with which attackers may exploit a finding. It takes into account the level of access required, availability of exploitation information, requirements relating to social engineering, race conditions, brute forcing, etc, and other impediments to exploitation.

High Attackers can unilaterally exploit the finding without special permissions or significant roadblocks.

Medium Attackers would need to leverage a third party, gain non-public information, exploit a race condition, already have privileged access, or otherwise overcome moderate hurdles in order to exploit the finding.

Low Exploitation requires implausible social engineering, a difficult race condition, guessing difficult-to-guess data, or is otherwise unlikely.

Category

[redacted] categorizes findings based on the security area to which those findings belong. This can help organizations identify gaps in secure development, deployment, patching, etc.

Access Controls	Related to authorization of users, and assessment of rights.
Auditing and Logging	Related to auditing of actions, or logging of problems.
Authentication	Related to the identification of users.
Configuration	Related to security configurations of servers, devices, or software.
Cryptography	Related to mathematical protections for data.
Data Exposure	Related to unintended exposure of sensitive information.
Data Validation	Related to improper reliance on the structure or values of data.
Denial of Service	Related to causing system failure.
Error Reporting	Related to the reporting of error conditions in a secure fashion.
Patching	Related to keeping software up to date.
Session Management	Related to the identification of authenticated users.
Timing	Related to race conditions, locking, or order of operations.

Appendix B: Project Contacts

[redacted]