



**SCADAfence**

# **A Comprehensive Guide to Industrial Device Patching**

**--- Public Preview ---**

A SCADAfence Research Original Publication

Ofer Shaked, Co-Founder and CTO, SCADAfence

# Ofer Shaked – Speaker Profile

- Co-Founder & CTO of SCADAfence
- 13 years background in SCADA / Industrial Security
- Ex-officer in the Israeli Intelligence Elite Cyber Unit
- Architect in the OTCSA
- Advisory Board member at ManuSec
- Speaker at ICS Security Conferences



# Table of Contents

01



Chapter 1

The Costs of Patching  
Vulnerability  
Discovery  
Patching Devices

02



Chapter 2

The Benefits of  
Patching

03



Chapter 3

Conclusions

04

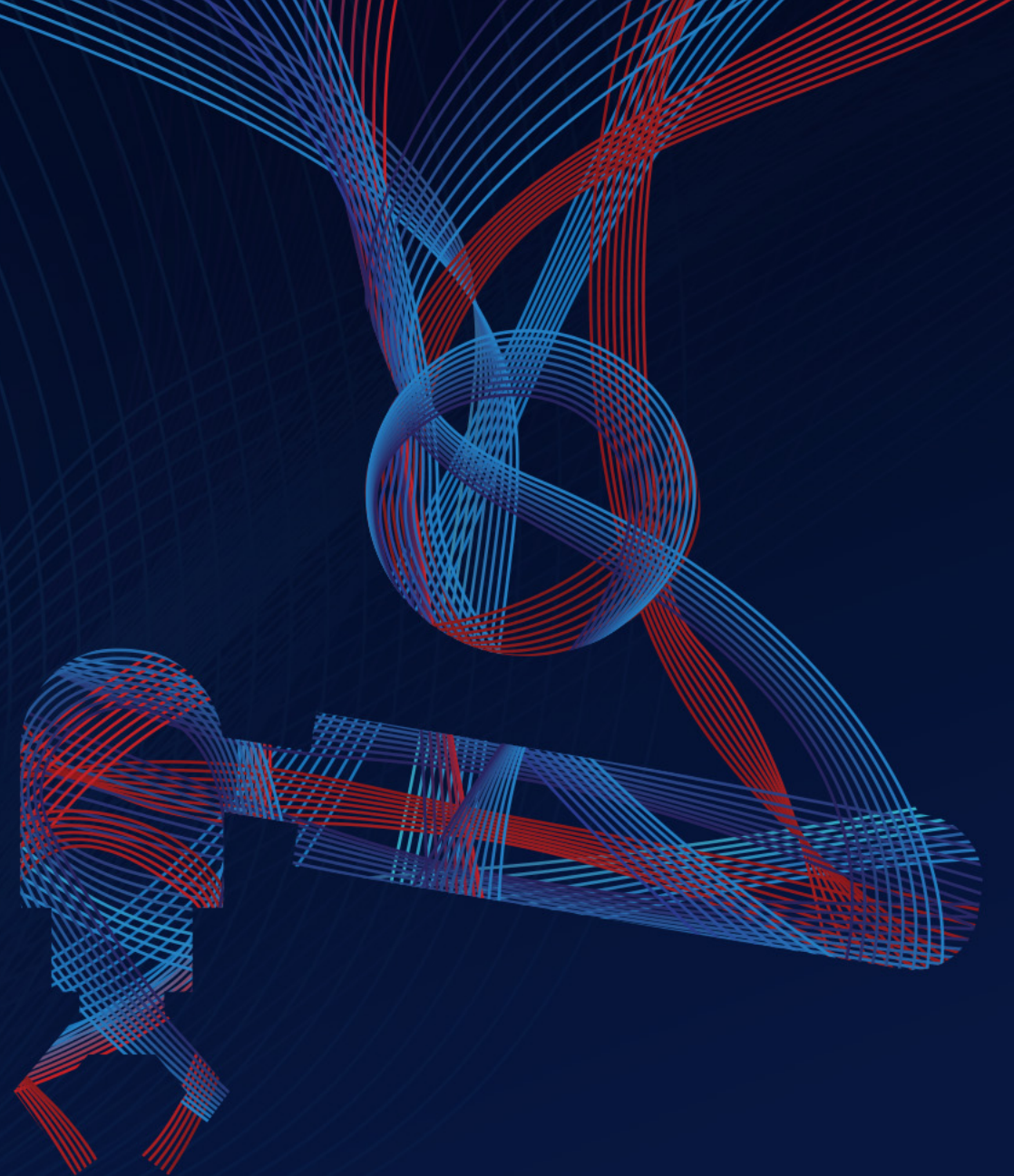


Chapter 4

A Decision Making Tool  
for Vulnerability  
Management

# The Cost of Patching

Step 1: Vulnerability Discovery



# Industrial Device Vulnerability Management Processes

To know if you have a vulnerability, you first need to discover all your assets. You then need to assess them for vulnerabilities.



# Case Studies: Vulnerability Scanning

## Case Study #1

### Automotive Manufacturer in Germany

Critical servers crashed in production from scanning for one critical vulnerability. The servers were a key part of the manufacturing process and their failure caused downtime.

Cause: The scanner opened 13 sockets while the servers only supported up to 4 sockets in parallel.

## Case Study #2

### BMS Operator in the US

Over 50% of the building automation systems crashed as a result of a network-wide scan using one of the top 3 Vulnerability Scanners.

Fixing it required calling technicians from multiple vendors to the affected sites.

Monetary cost to repair - \$1Million.

Cause: The scanner triggered a functionality that isn't in common use and wasn't properly tested on the target devices by the vendors.

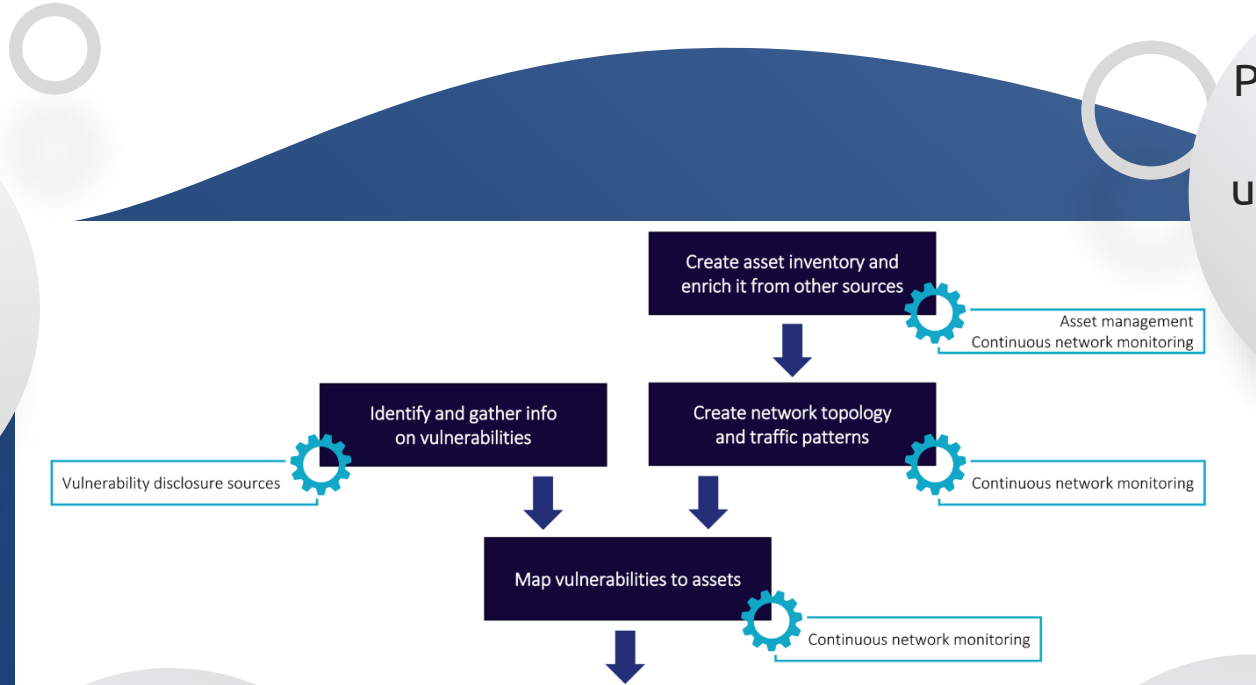
## Conclusion

**Vulnerability scanning is unfit for scanning in OT.**



# Four Steps To Safe Vulnerability Discovery

**Step 1:**  
Create an Asset Inventory  
(passive & active sources).



**Step 2:**  
Perform Network Mapping to understand which assets are reachable and from where.

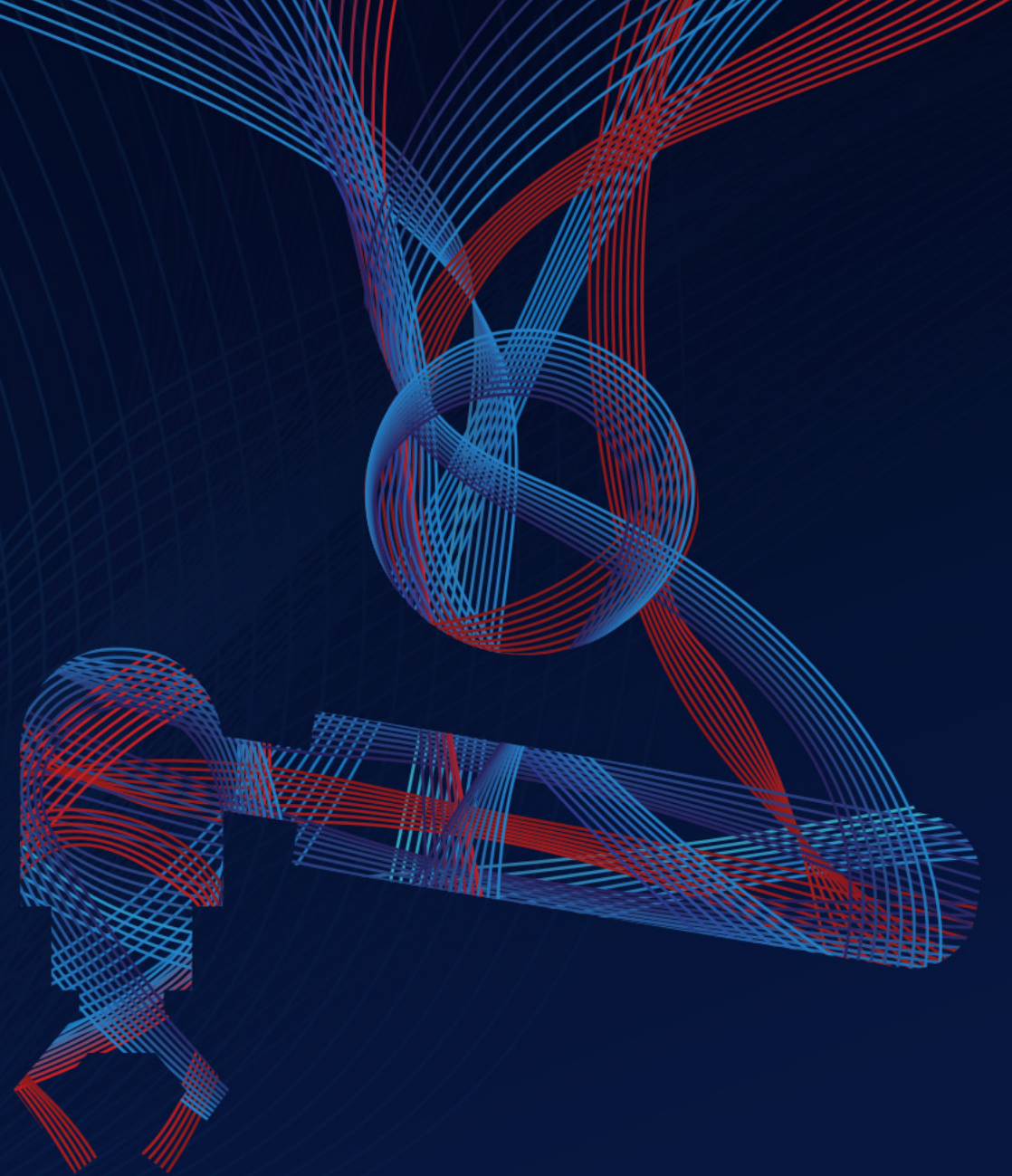
**Step 3:**  
Gather vulnerabilities from vulnerability disclosure sources.

**Step 4:**  
Map vulnerabilities to assets.

Source: OTCSA Position Paper: "Vulnerability Management for Operational Technology"

# The Cost of Patching

Step 2: Patching Devices





# How Many Patches are Required Per Device?

## Case Study: Siemens SIMATIC S7-1500 CPU

The screenshot shows the Siemens Security Advisories search interface. The search term 's7-1500 cpu' is entered in the search bar. The results table shows 23 entries, with the first 15 displayed. The second entry, 'Denial-of-Service Vulnerabilities in SIMATIC S7-1500 CPU Family', is highlighted. The search results are filtered to show 15 of 23 entries.

ID	CVSS Score	Document Title	Info	Version	Last Update	Download
SSA-179516	5.9	OpenSSL Vulnerability in Industrial Products	i	V1.6	2020-02-10	PDF TXT
SSA-180635	7.5	Denial-of-Service Vulnerabilities in SIMATIC S7-1500 CPU Family	i	V1.1	2020-02-10	PDF TXT
SSA-307392	7.5	Denial-of-Service in OPC UA in Industrial Products	i	V1.6	2020-03-10	PDF TXT
SSA-616472	6.5	ZombieLoad and Microarchitectural Data Sampling Vulnerabilities in Industrial Products	i	V1.6	2020-03-10	PDF TXT

Showing 1 - 15 from 23 entries (Filtered)

Source: Siemens Security Advisories



23 Security Advisories

Siemens SIMATIC S7-1500 CPU – 23 security advisories

83% Require Patching

19 out of the 23 Entries are CPU vulnerabilities that require patching

Multiple Vulnerabilities

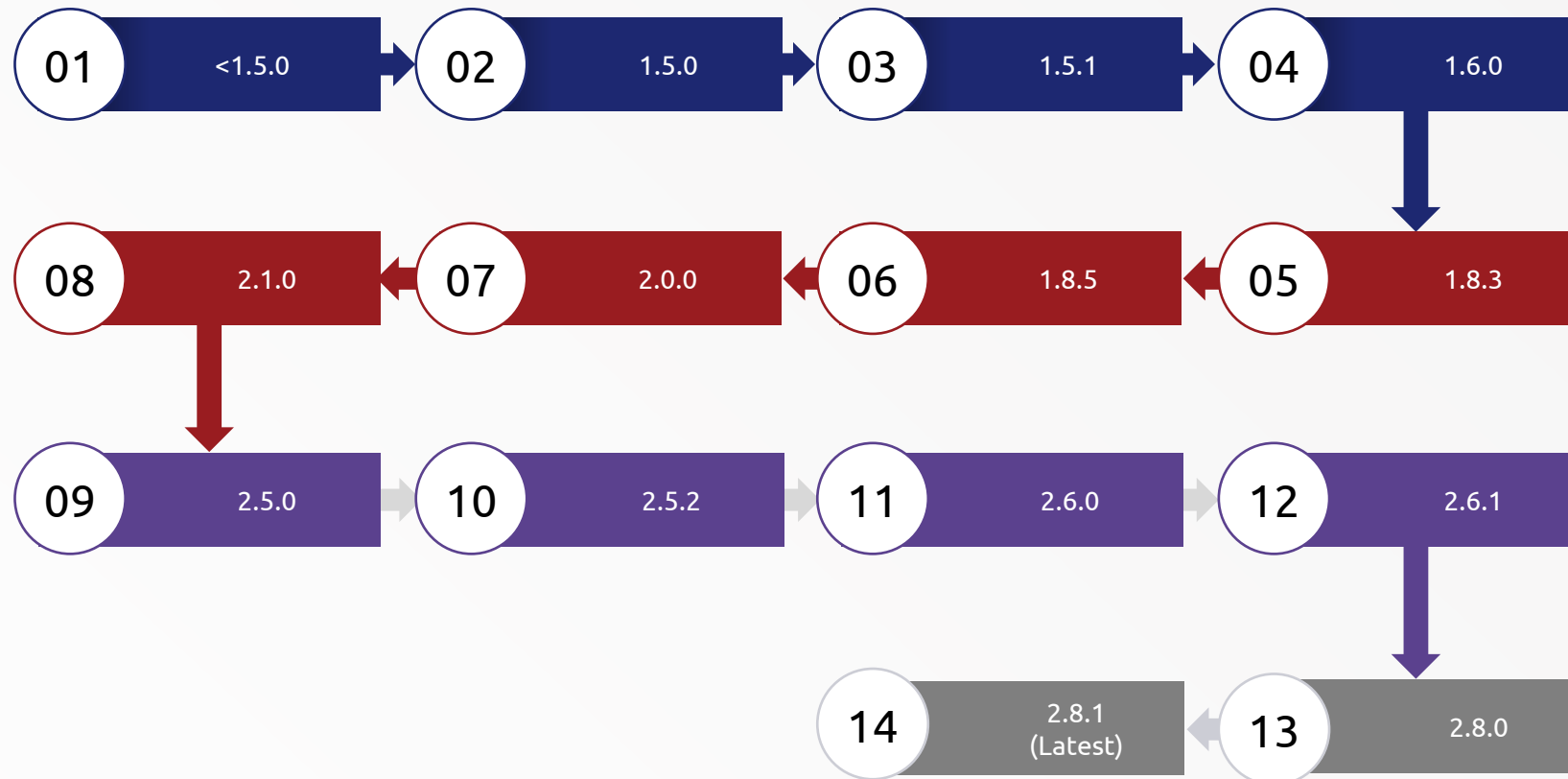
Some of the 19 entries contain multiple vulnerabilities

Notice

The product is used as an example to an industry-wide problem, it is not specific to one product or vendor.

# Siemens SIMATIC S7-1500 CPU – Required Security Patches

In 7 years since its launch, 13 updates per S7-1500 device were required, in order to stay fully patched.



**Conclusion: Staying fully patched requires frequent attention per device.**

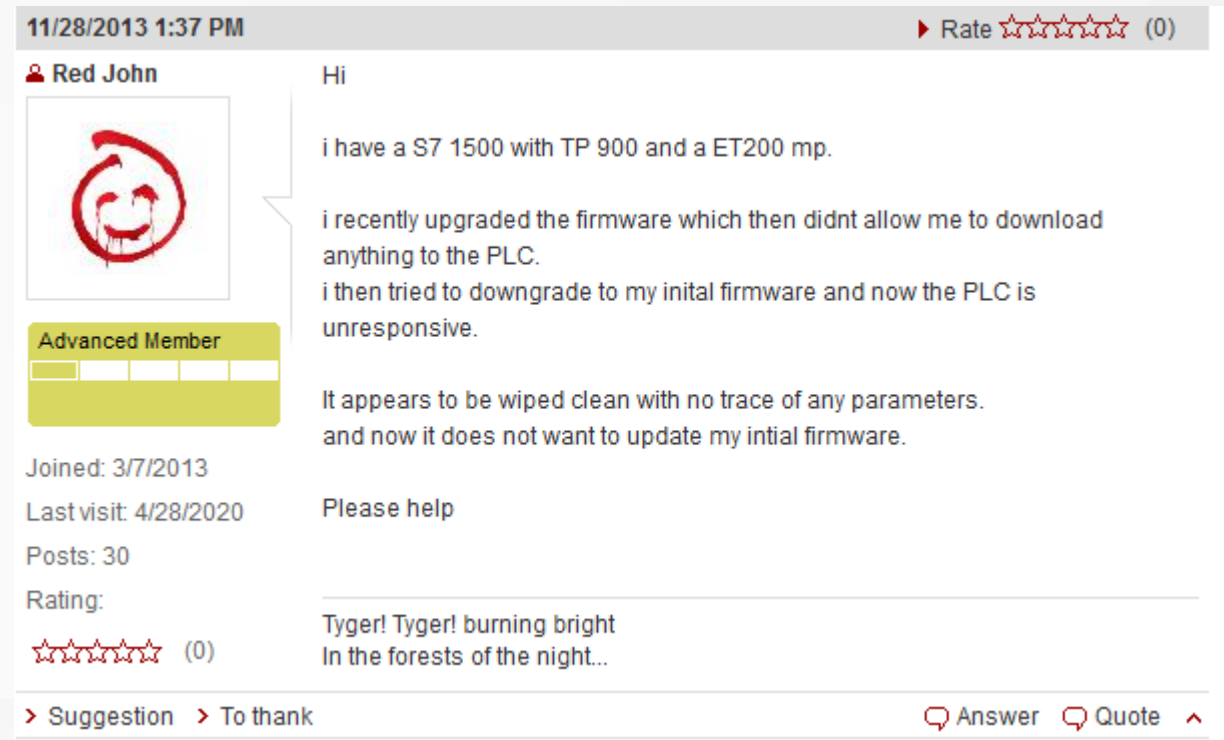
# The Cost of Applying Patches - #1

## Upgrade Failure

A user tried to upgrade the firmware on a Siemens SIMATIC S7-1500 CPU, resulting in an error in downloading programming into the PLC.


## Downgrade Failure

When the user tried to downgrade – he bricked the device.



11/28/2013 1:37 PM ▶ Rate ☆☆☆☆☆ (0)

**Red John**



Advanced Member

Joined: 3/7/2013  
Last visit: 4/28/2020  
Posts: 30  
Rating: ☆☆☆☆☆ (0)

Hi

i have a S7 1500 with TP 900 and a ET200 mp.

i recently upgraded the firmware which then didnt allow me to download anything to the PLC.  
i then tried to downgrade to my inital firmware and now the PLC is unresponsive.

It appears to be wiped clean with no trace of any parameters.  
and now it does not want to update my inital firmware.

Please help

---

Tyger! Tyger! burning bright  
In the forests of the night...

> Suggestion > To thank Answer Quote ^



Interested in learning  
more?

Get the full guide & 3  
Decision Making tools here  
for free:

[https://l.scadafence.com/  
industrial-device-patching-  
costs-vs-benefit](https://l.scadafence.com/industrial-device-patching-costs-vs-benefit)