Project Achilles

Novel Vulnerability Management System

Whois

Ing. Adrián Ondov

- **Vulnerability Management**
- **Cyber Threat Intelligence**

(+ *casual Achilles user*)

CSIRT.SK

Background

1. Cyber Security in Public Sector of SVK
2. Responsible for > 8 200 institutions

What is Project Achilles?

Combination of:

1. Open-source SW: ELK stack
2. Proprietary SW: Nessus, The Hive, Cortex
3. Interconnected by **Cyber Operations Center** (COC)

Stack

Nessus®
vulnerability scanner

TheHive

Cortex

Achilles

Goals

1. Identification of Attack Surface
2. Early Warning Capabilities
3. Remediation of Identified Vulnerabilities
4. Attack Surface Reduction

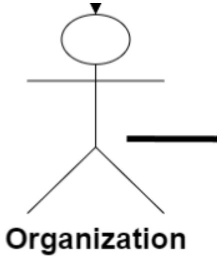
! Cyber Attack Prevention !

Achilles

Constituency Registry - VISKB

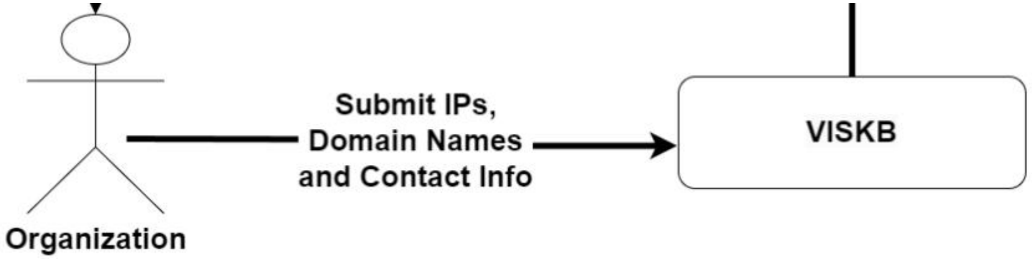
1. Organizational information
2. Contact information
   - Roles
   - E-mails
   - Phone numbers
3. IP addresses
4. Domain names
5. Network services

The Idea



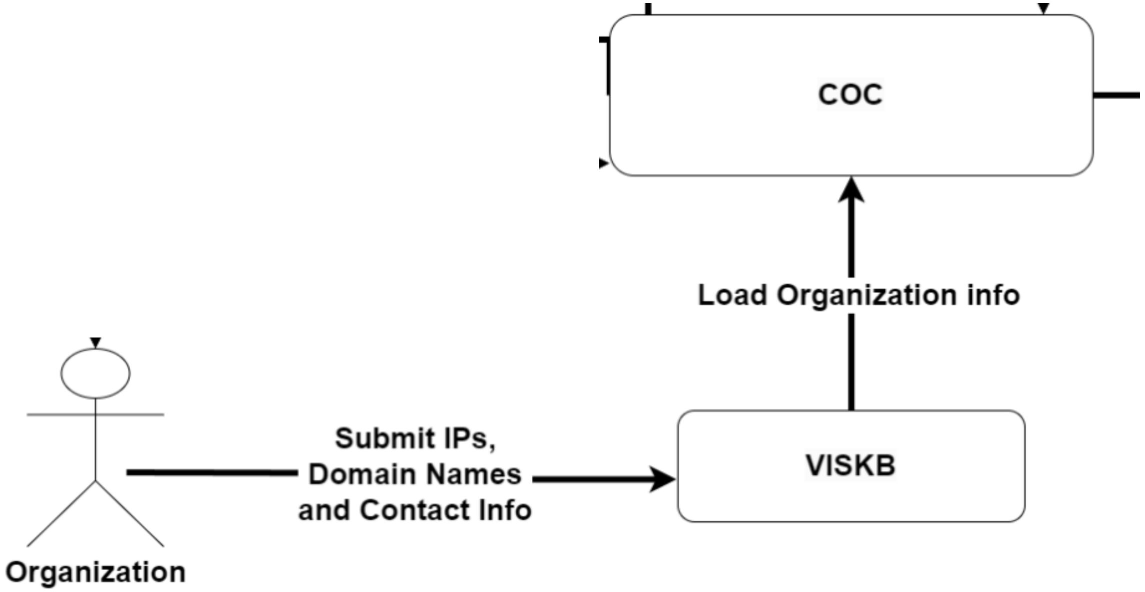
Achilles

The Idea



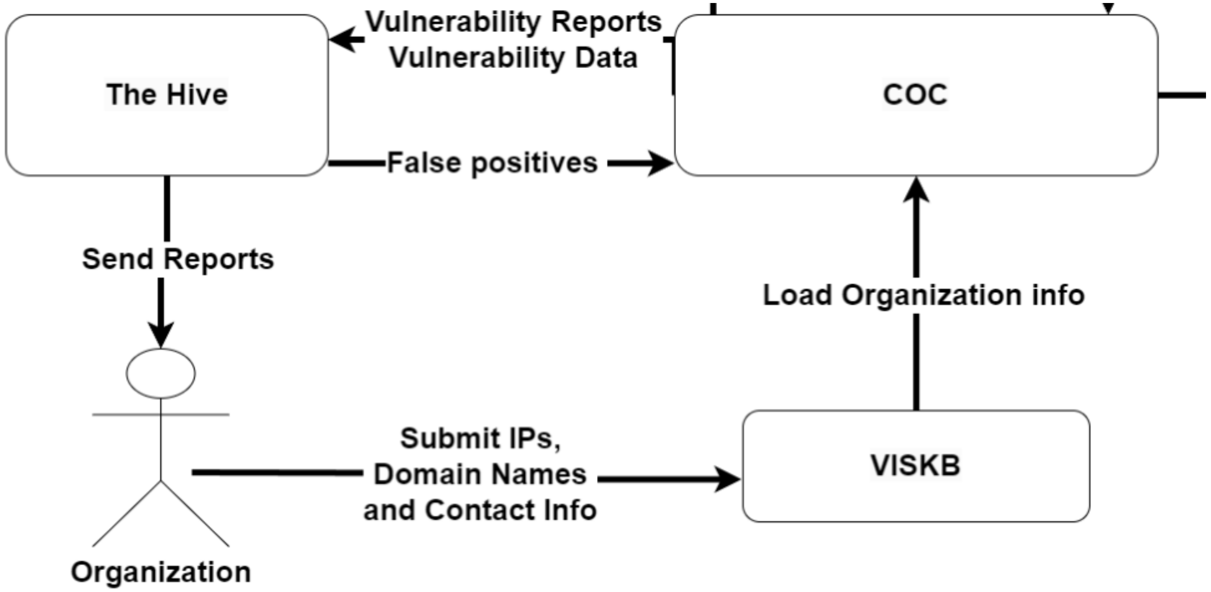
Achilles

The Idea



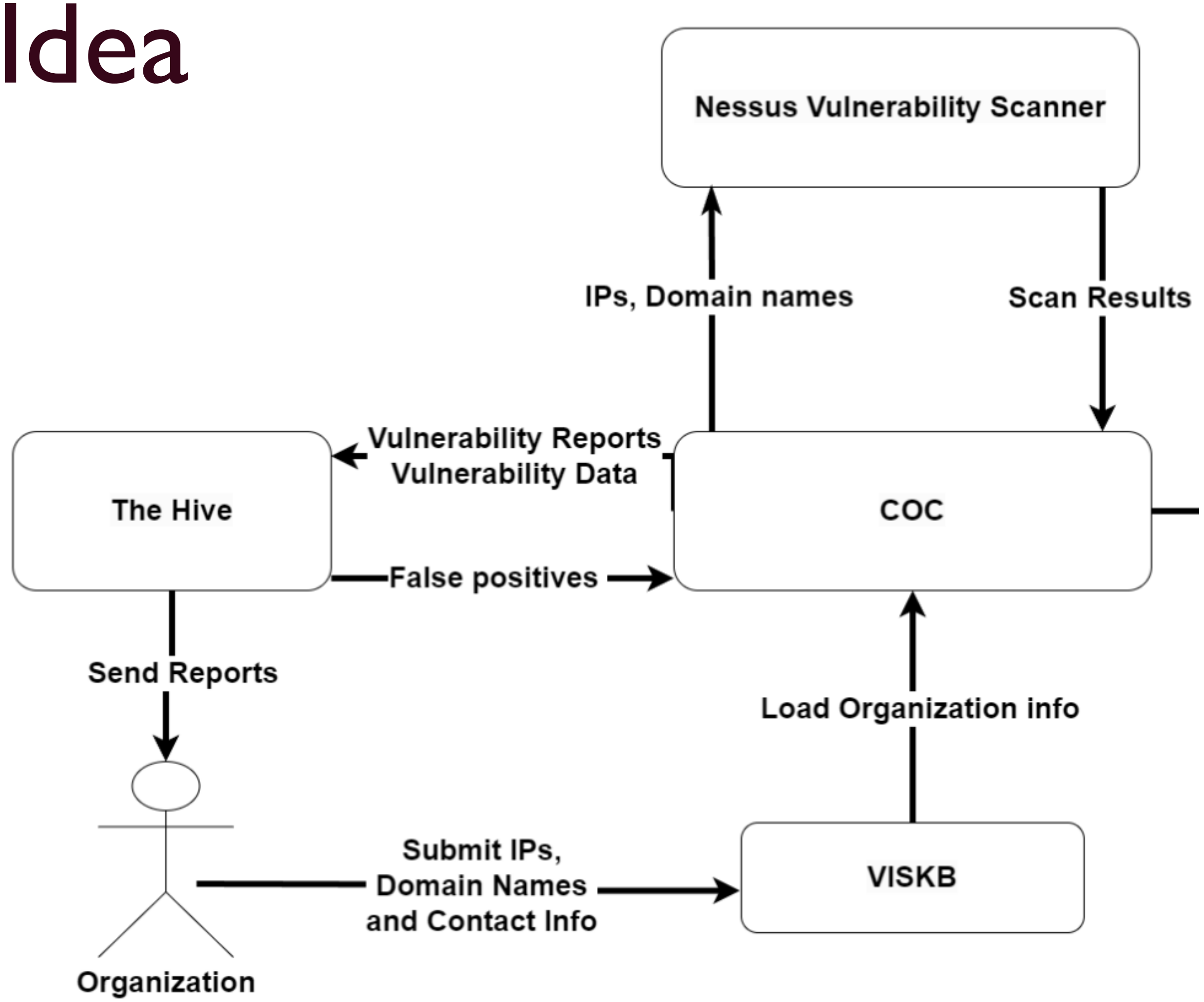
Achilles

The Idea



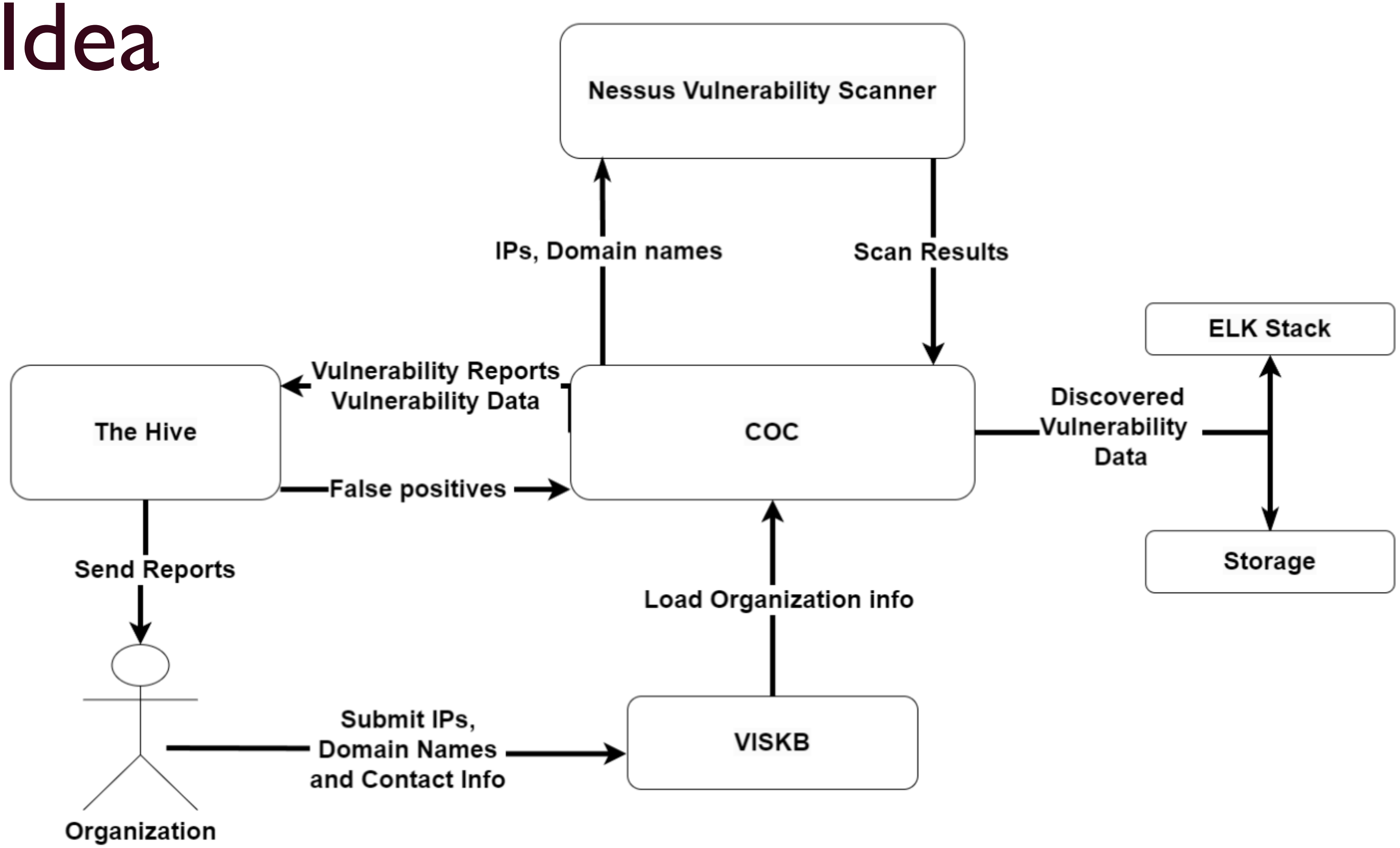
Achilles

The Idea



Achilles

The Idea



Achilles

How Does It Work?

0. Register organization in VISKB

Achilles

How Does It Work?

0. Register organization in VISKB

1. Organization submits:
   - Contact information
   - PGP/Encryption key
   - Domain names, IPs
   - *Whitelists our Scanner / Informs their SOC*

Achilles

How Does It Work?

0. Register organization in VISKB

1. Organization submits:
   - Contact info
   - PGP/Encryption key
   - Domain names, IPs
   - *Whitelists our Scanner / Informs their SOC'*

2. Run scan, discover vulnerabilities → Nessus® vulnerability scanner

Achilles

How Does It Work?

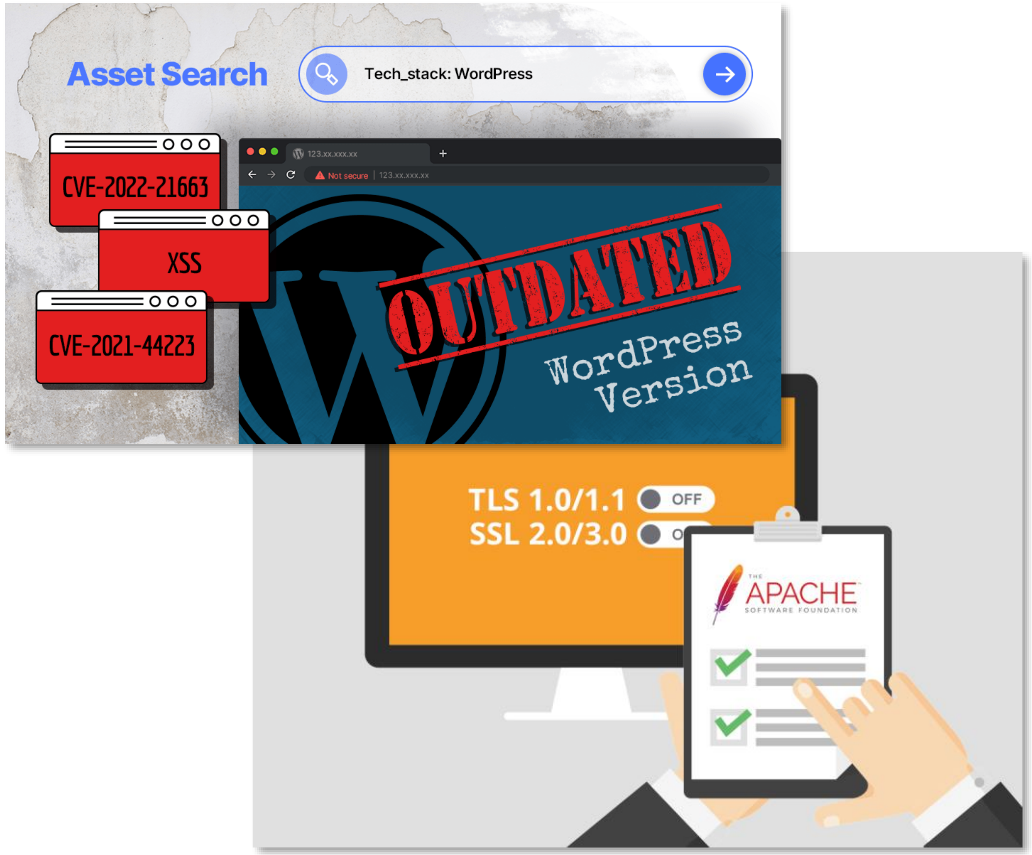
0. Register organization in VISKB
1. Organization submits:
   - Contact info
   - PGP/Encryption key
   - Domain names, IPs
   - *Whitelists our Scanner / Informs their SOC*
2. Run scan, discover vulnerabilities →

   Nessus®
   vulnerability scanner
3. Send PDF report with findings

Achilles

What We Hunt For?

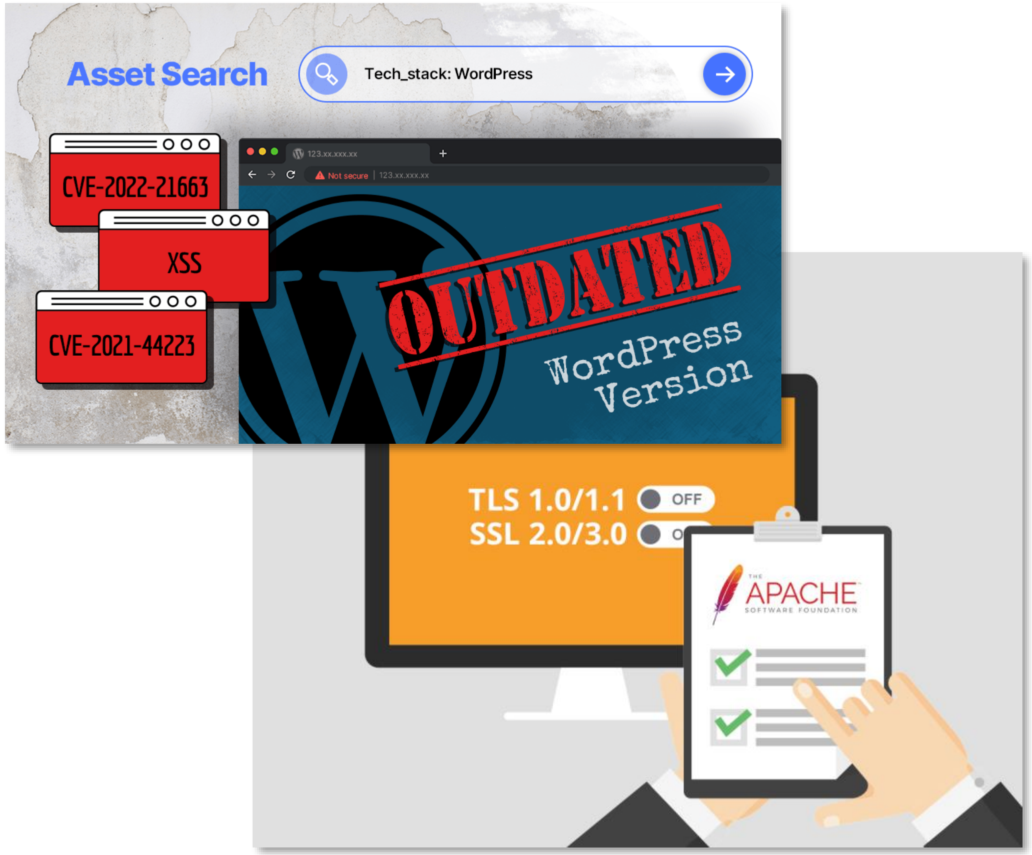
1. Vulnerable or Outdated SW
   - Web server
   - Wordpress
   - Joomla
   - Drupal
   - Mail server
   - …



Achilles

What We Hunt For?

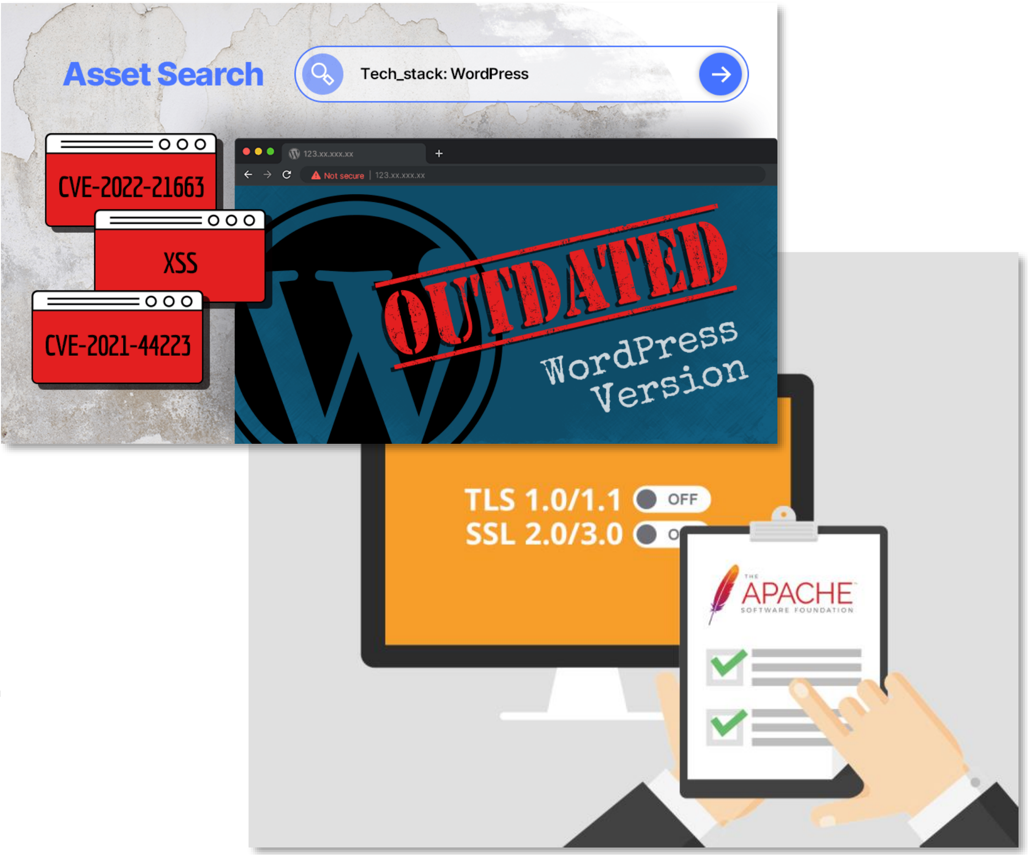
1. Vulnerable or Outdated SW
   - Web server
   - Wordpress
   - Joomla
   - Drupal
   - Mail server
   - …
2. Old/Missing TLS/SSL



Achilles

What We Hunt For?

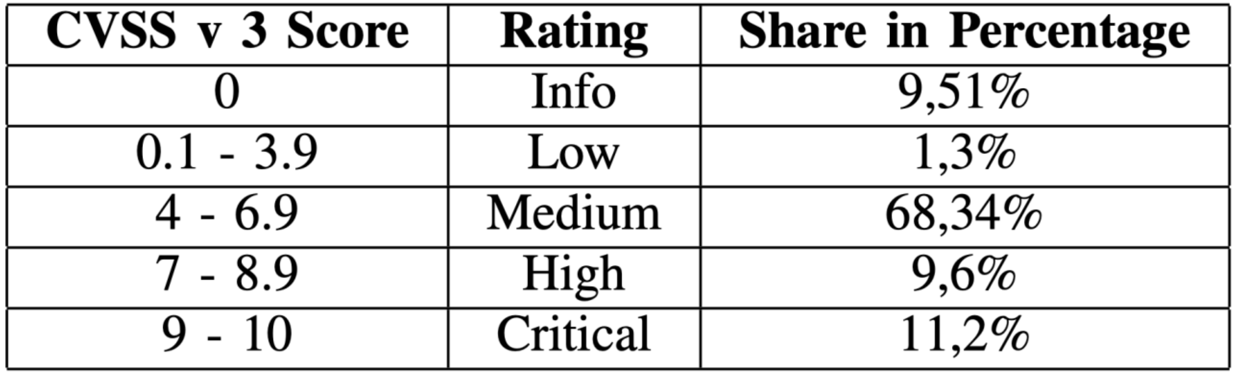
1. Vulnerable or Outdated SW
   - Web server
   - Wordpress
   - Joomla
   - Drupal
   - Mail server
   - …
2. Old/Missing TLS/SSL
3. Website unreachability – 503, 504



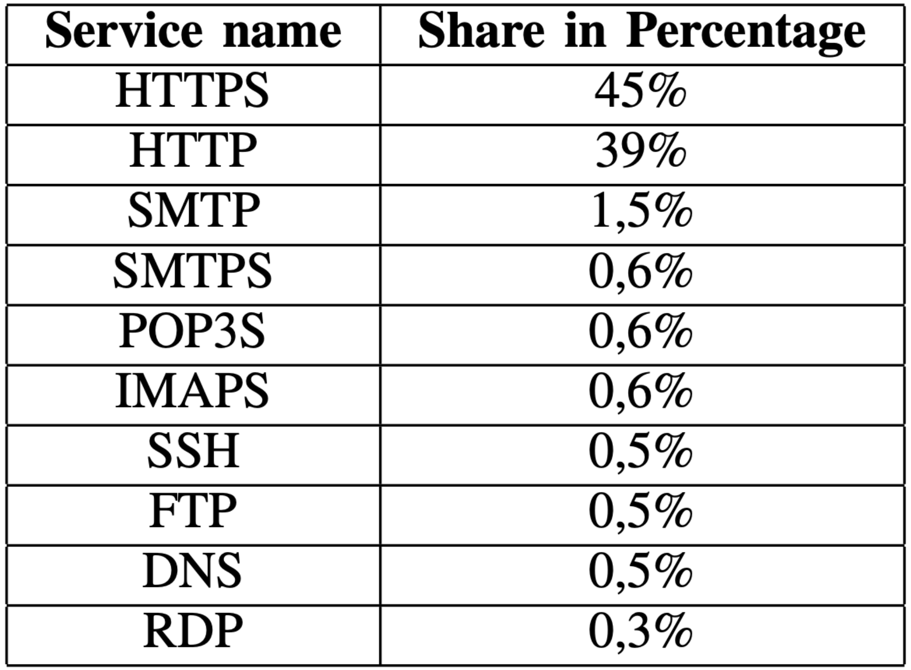
Achilles

What We Discovered?

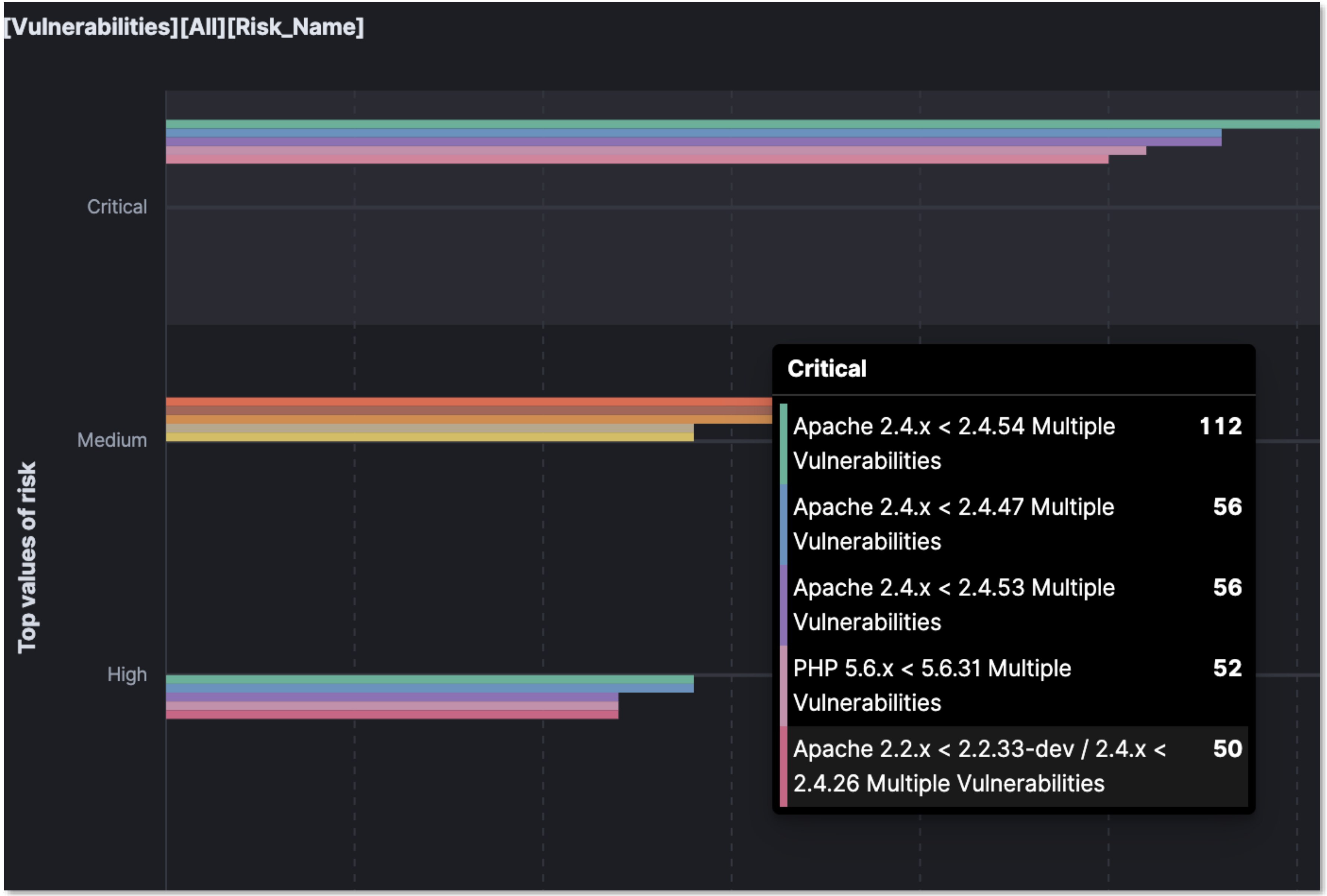
1. We scanned > 26 000 IPs or domains
2. Discovered > 45 000 vulnerabilities
3. Identified services provided by our constituents



CVSS v 3 Score	Rating	Share in Percentage
0	Info	9,51%
0.1 - 3.9	Low	1,3%
4 - 6.9	Medium	68,34%
7 - 8.9	High	9,6%
9 - 10	Critical	11,2%



Service name	Share in Percentage
HTTPS	45%
HTTP	39%
SMTP	1,5%
SMTPS	0,6%
POP3S	0,6%
IMAPS	0,6%
SSH	0,5%
FTP	0,5%
DNS	0,5%
RDP	0,3%

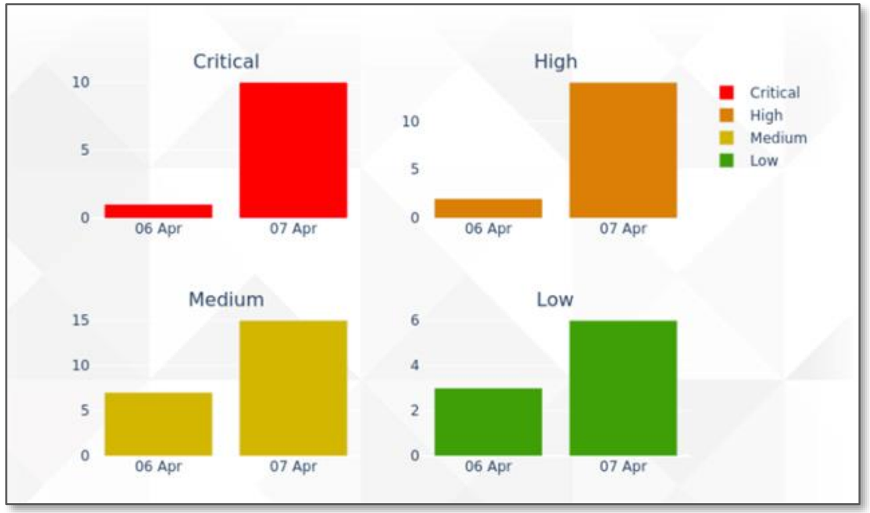


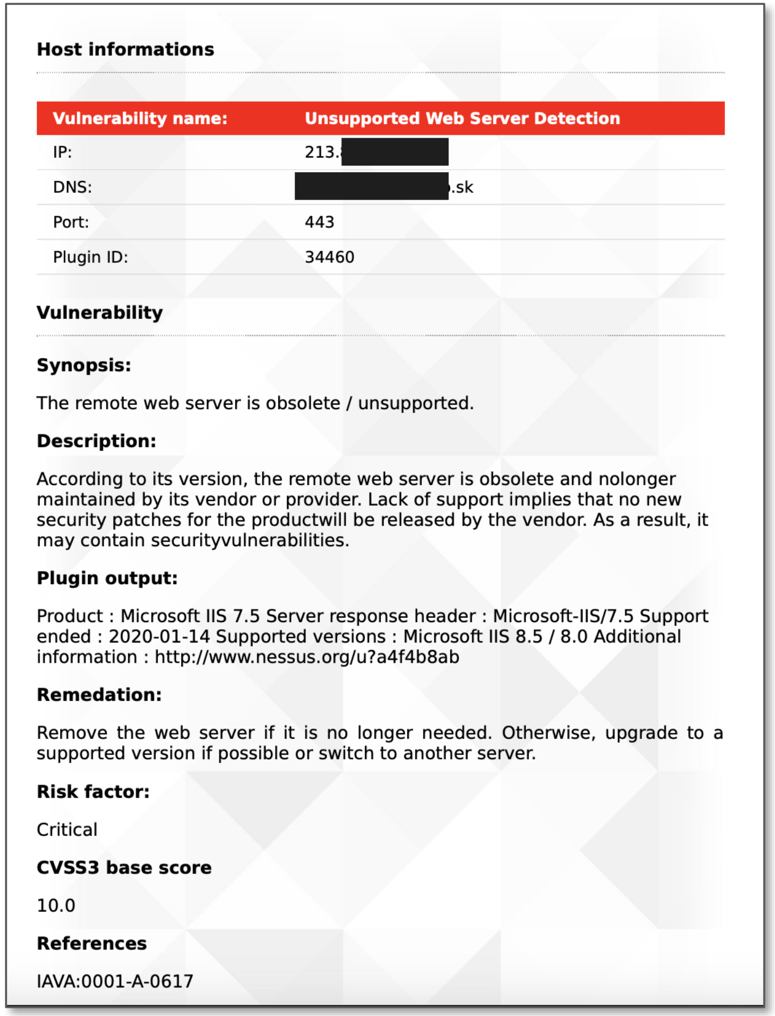
Critical	
Apache 2.4.x < 2.4.54 Multiple Vulnerabilities	112
Apache 2.4.x < 2.4.47 Multiple Vulnerabilities	56
Apache 2.4.x < 2.4.53 Multiple Vulnerabilities	56
PHP 5.6.x < 5.6.31 Multiple Vulnerabilities	52
Apache 2.2.x < 2.2.33-dev / 2.4.x < 2.4.26 Multiple Vulnerabilities	50

Achilles

Communicating Findings

1. E-mail PDF report with identified vulnerabilities
2. Vulnerability evolution data





Host informations

Vulnerability name:	Unsupported Web Server Detection
IP:	213.[redacted]
DNS:	[redacted].sk
Port:	443
Plugin ID:	34460

Vulnerability

Synopsis:

The remote web server is obsolete / unsupported.

Description:

According to its version, the remote web server is obsolete and nolonger maintained by its vendor or provider. Lack of support implies that no new security patches for the productwill be released by the vendor. As a result, it may contain securityvulnerabilities.

Plugin output:

Product : Microsoft IIS 7.5 Server response header : Microsoft-IIS/7.5 Support ended : 2020-01-14 Supported versions : Microsoft IIS 8.5 / 8.0 Additional information : http://www.nessus.org/u?a4f4b8ab

Remedation:

Remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server.

Risk factor:

Critical

CVSS3 base score

10.0

References

IAVA:0001-A-0617

Achilles

Common Responses

1. [redacted]
2. [redacted]
3. [redacted]
4. [redacted]

Achilles

Common Responses

1. None, no response ☹
2. [redacted]
3. [redacted]
4. [redacted]

Achilles

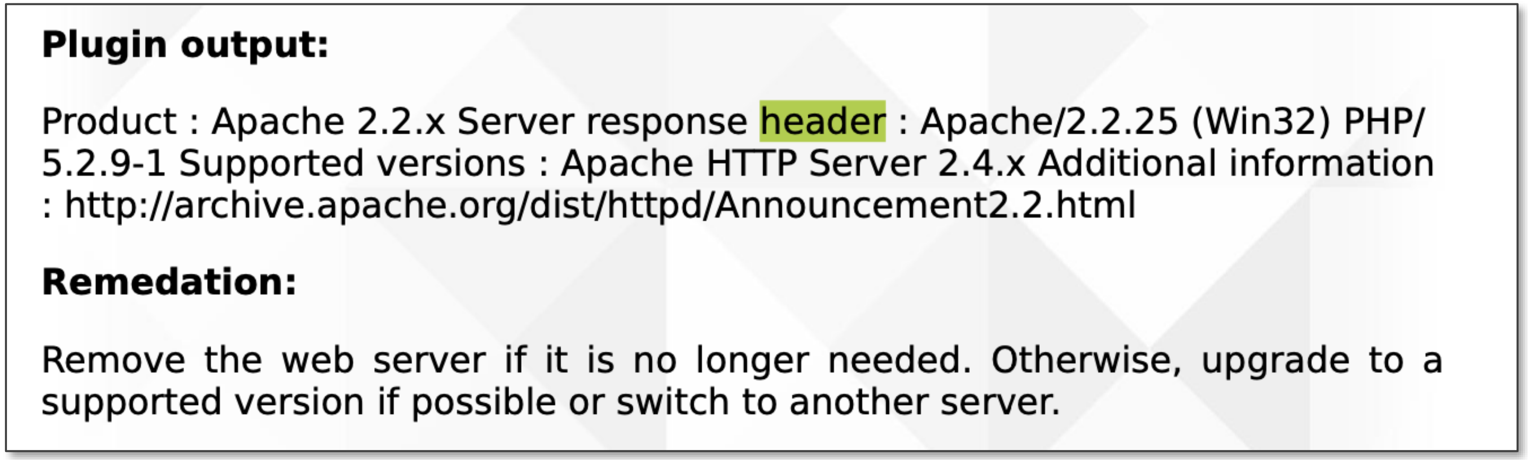
Common Responses

1. None, no response ☹
2. We know, but can't fix it 😐
3. [redacted]
4. [redacted]

Achilles

Common Responses

1. None, no response ☹
2. We know, but can’t fix it 😐
3. Removed the header – please rescan ☺
4. [redacted]



Plugin output:

Product : Apache 2.2.x Server response header : Apache/2.2.25 (Win32) PHP/5.2.9-1 Supported versions : Apache HTTP Server 2.4.x Additional information : http://archive.apache.org/dist/httpd/Announcement2.2.html

Remedation:

Remove the web server if it is no longer needed. Otherwise, upgrade to a supported version if possible or switch to another server.

Achilles

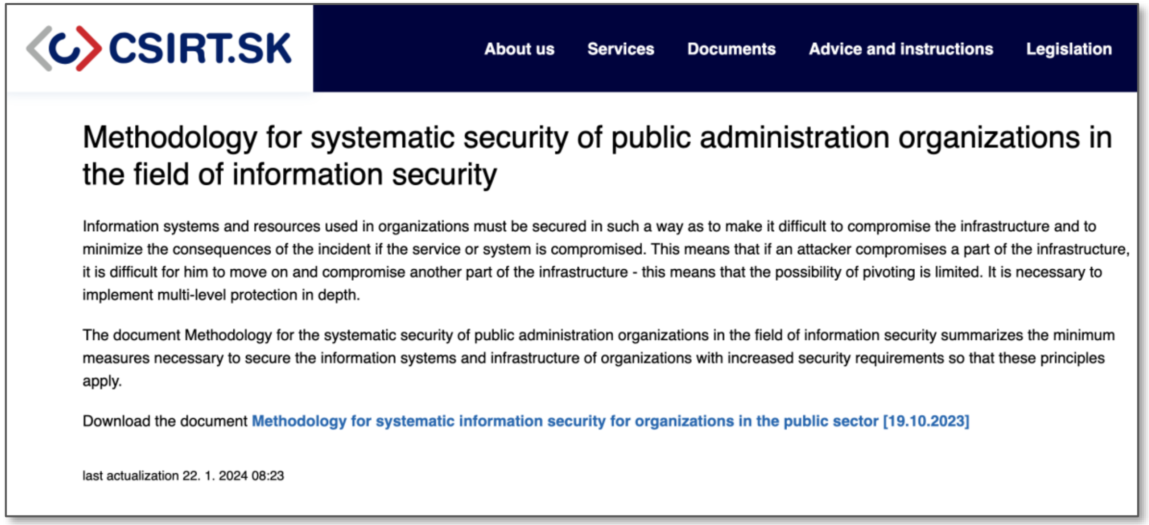
Common Responses

1. None, no response ☹
2. We know, but can’t fix it 😐
3. Removed the header – please rescan ☺
4. Thank you, we fixed it, here are more IPs ☺☺☺

Secondary Activities

Communicating Findings 2.0

1. Tailored webserver hardening guides
2. Regular warning posts
3. Trainings for constituents



Methodology for systematic security of public administration organizations in the field of information security

Information systems and resources used in organizations must be secured in such a way as to make it difficult to compromise the infrastructure and to minimize the consequences of the incident if the service or system is compromised. This means that if an attacker compromises a part of the infrastructure, it is difficult for him to move on and compromise another part of the infrastructure - this means that the possibility of pivoting is limited. It is necessary to implement multi-level protection in depth.

The document Methodology for the systematic security of public administration organizations in the field of information security summarizes the minimum measures necessary to secure the information systems and infrastructure of organizations with increased security requirements so that these principles apply.

Download the document Methodology for systematic information security for organizations in the public sector [19.10.2023]

last actualization 22. 1. 2024 08:23

Secondary Activities

Additional Achilles Tasks

- **DoS detection** – routinely GETting webservers
- Service categorization (internally)
- Tracking false positives
- Tracking self-discovered vulnerabilities

Benefits so Far?

1. > 400 of removed critical vulnerabilities
2. > 45 000 identified vulnerabilities
3. Shorter incident resolution time
4. Improved communication with constituents
5. Better visibility

Future Work and Plans?

1. Increasing the frequency of scanning
2. Including more targetted scanners
3. Concurrent scanning
4. Making source code Open-Source

Lessons Learned

1. We don't have a problem with vulnerabilities – we have a problem with people
2. Nessus is (un)surprisingly accurate (< 0.01% False Positives)
3. Reactivity = *Good*, Proactivity = *Better*, Both = *The Best*
4. Better to be safe than sorry

Q&A