Proactive Cyber Threat Management with SploitScan

IIA Norway Risk Roundtable November 22, 2024

Your IIA Norway Risk Roundtable Hosts:

The Institute of Internal Auditors Norge

Ellen Brataas, CEO IIA Norway

Ellen has extensive industry and consulting experience across domains like risk management, internal audit and IT resilience. As CEO of IIA Norway she is continuously advancing GRC best practice and readiness in Scandinavia through peer exchanges, expert blogs and training.

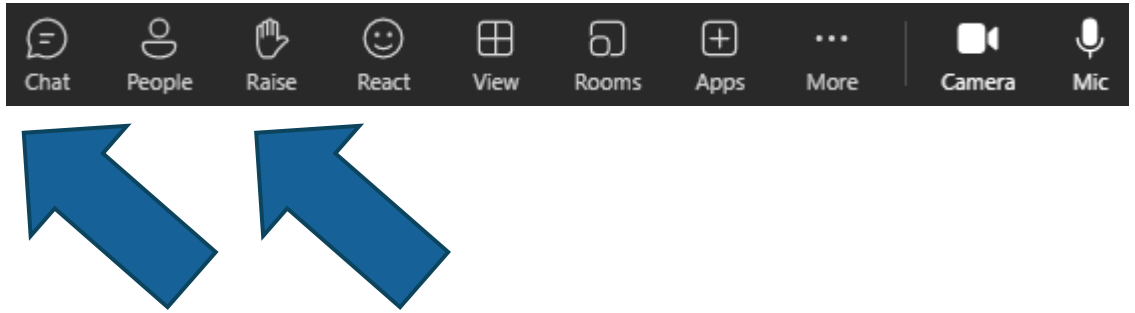
Alexander Hagenah, GRC Head Cyber Controls at SIX

Alex has over 20 years in cybersecurity, which encompasses, ethical hacking, offensive security and devising cybersecurity strategies on a global scale.
With his experience across sectors, he brings agility and an innovative lens to risk management considerations in changing environments.

Some Housekeeping:

- A recording of the session will be made available to registrants and participants.
- The lines are muted but this session will be interactive throughout.
- Please raise your hand if you want to ask a question or add a comment.

Participation Options



Threat Detection & Prevention Expectations by Regulators in Europe

"Member States should encourage the use of any innovative technology, including artificial intelligence, the use of which could improve the detection and prevention of cyberattacks..."

NIS2: Preamble (51)

"Financial entities shall have in place mechanisms to promptly detect anomalous activities..."

EU DORA: Article 10

"Undertakings shall continuously monitor their critical national information systems to prevent, detect and counter incidents which may harm national security interests."

Norwegian National Security Act: Section 6-4

"Identification of the institution-specific threat landscape..."
"Response to identified vulnerabilities and cyber attacks..."

FINMA Circular 2023/1: Cyber Risk Management

Issues with CVE Management today:

America's Cyber Defense Agen

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESIL

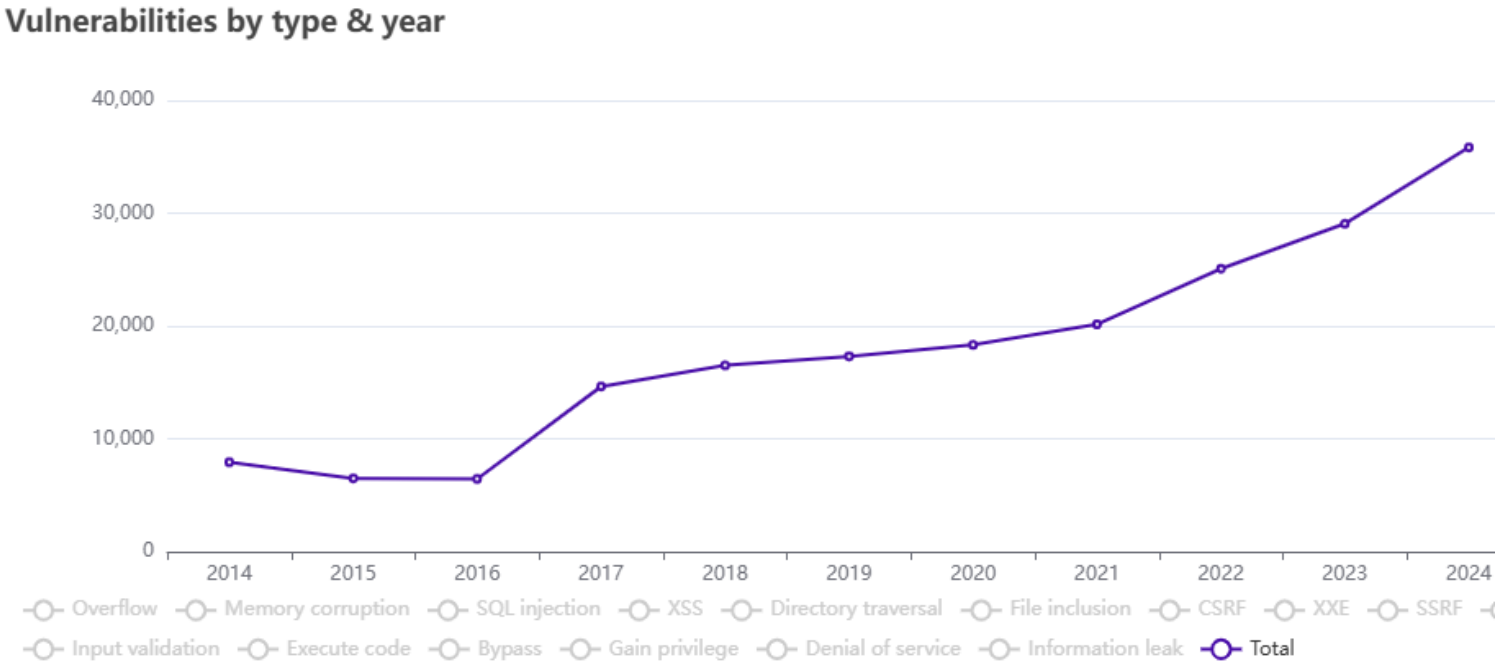
CVE-2024-20481

Cisco ASA and FTD Denial-of-Service Vulnerability: *Cisco Adaptive Security Appliance (ASA) and Firepower Threa Defense (FTD) contain a missing release of resource after effective lifetime vulnerability that could allow an unauthenticated, remote attacker to cause a denial-of-service (DoS) of the RAVPN service.*

Known To Be Used in Ransomware Campaigns? **Unknown**

Action: Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

- **Date Added:** 2024-10-24
- **Due Date:** 2024-11-14



CVE Volume

Deficiencies:
Workflow
Prioritisation
Assurance

It's 5pm.

Do you know where your critical vulnerabilities are?

Are the issues raised within your company and resolved?

Source: Cyber Risk Management deficiencies identified in the SEC's SolarWinds complaint and charge Oct. 2023.

SploitScan

Benefits:
Workflow: Improved CVE Handling through Data Aggregation
Prioritisation: Risk-based CVE Filtering and Mitigation
Assurance: CVE Oversight for Regulatory & Business Compliance

SploitScan

❓ Why

- **Vulnerability Management in Organizations**
  - Thousands of vulnerabilities
  - Usually depending on CVSS Score
  - Business needs to adjust

- **But what does really matter?**
  - Critical functions and important business services (3rd party risk management)
  - Is it the asset on the publicly accessible / on the internet?
  - Are threat actors exploiting the vulnerabilities?
  - Are exploits public for anyone to use?

- **We want to achieve better judgement on vulnerabilities and their respective impact**

SploitScan

🌟 Features

- **CVE Information Retrieval:** Fetches CVE details from the National Vulnerability Database.
- **EPSS Integration:** Includes Exploit Prediction Scoring System (EPSS) data, offering a probability score for the likelihood of CVE exploitation, aiding in prioritization.
- **Public Exploits Aggregation:** Gathers publicly available exploits, enhancing the understanding of vulnerabilities.
- **CISA KEV:** Shows if the CVE has been listed in the Known Exploited Vulnerabilities (KEV) of CISA.
- **Patching Priority System:** Evaluates and assigns a priority rating for patching based on various factors including public exploits availability.
- **AI-Powered Risk Assessment:** Leverages OpenAI to provide detailed risk assessments, potential attack scenarios, mitigation recommendations, and executive summaries.
- **Multi-CVE Support** and Export Options
- **Vulnerability Scanner Import:** Import vulnerability scans from popular vulnerability scanners and search directly for known exploits.
- **User-Friendly Interface:** Easy to use, providing clear and concise information.

SploitScan

🚀 Demo

```
 ____  ____  _     ___ _____ ____   ____    _    _   _
/ ___||  _ \| |   / _ \_   _/ ___| / ___|  / \  | \ | |
\___ \| |_) | |  | | | || | \___ \| |     / _ \ |  \| |
 ___) |  __/| |__| |_| || |  ___) | |___ / ___ \| |\  |
|____/|_|   |_____\___/ |_| |____/ \____/_/   \_\_| \_|

v0.11.0 / Alexander Hagenah / @xaitax / ah@primepage.de

CVE ID: CVE-2024-28995

┌──[ 🔍 Vulnerability information ]
│
├ Published:   2024-06-06
├ Base Score:  8.6 (HIGH)
├ Vector:      CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N
└ Description:    SolarWinds Serv-U was susceptible to a directory transversal vulnerability that would allow
              access to read sensitive files on the host machine.

┌──[ 💣 Public Exploits (Total: 17) ]
│
├ GitHub
│  ├ Date: 2024-08-25 - https://github.com/gotr00t0day/CVE-2024-28995
│  ├ Date: 2024-07-01 - https://github.com/Stuub/CVE-2024-28995
│  ├ Date: 2024-06-26 - https://github.com/Praison001/CVE-2024-28995-SolarWinds-Serv-U
│  ├ Date: 2024-06-17 - https://github.com/muhammetali20/CVE-2024-28995
│  ├ Date: 2024-06-15 - https://github.com/bigb0x/CVE-2024-28995
│  ├ Date: 2024-06-14 - https://github.com/0xkucing/CVE-2024-28995
│  ├ Date: 2024-06-14 - https://github.com/krypton-kry/CVE-2024-28995
│  └ Date: 2024-06-13 - https://github.com/karkis3c/cves
│
├ VulnCheck
│  ├ Date: 2024-08-24 - https://github.com/gotr00t0day/CVE-2024-28995
│  ├ Date: 2024-07-01 - https://github.com/Stuub/CVE-2024-28995
│  ├ Date: 2024-06-26 - https://github.com/Praison001/CVE-2024-28995-SolarWinds-Serv-U
│  ├ Date: 2024-06-16 - https://github.com/muhammetali20/CVE-2024-28995
│  ├ Date: 2024-06-14 - https://github.com/bigb0x/CVE-2024-28995
│  ├ Date: 2024-06-14 - https://github.com/0xc4t/CVE-2024-28995
│  ├ Date: 2024-06-14 - https://github.com/huseyinstif/CVE-2024-28995-Nuclei-Template
│  ├ Date: 2024-06-14 - https://github.com/krypton-kry/CVE-2024-28995
│  └ Date: 2024-06-13 - https://github.com/karkis3c/cves
│
└ Other
   ├ PacketStorm: https://packetstormsecurity.com/search/?q=CVE-2024-28995
   └ Nuclei: https://raw.githubusercontent.com/projectdiscovery/nuclei-templates/main/http/cves/2024/CVE-2024-28995.yaml

┌──[ ∞ Exploit Prediction Score (EPSS) ]
│
└ EPSS Score:  96.00% Probability of exploitation.
```

SploitScan

Future

- **Standalone Web UI**
  - https://sploitscan.com (not functional yet)
  - Free for anyone to use
- **Monitoring capability**
  - Constantly check for new vulnerabilities
  - Constantly check for new exploits
- **Further enterprise tool integration**
  - Currently only Nessus Tenable, Rapid7 Nexpose, OpenVAS, Docker

Free Access to SploitScan and further information

https://github.com/xaitax/SploitScan	**SploitScan** is a free powerful and user-friendly tool designed by Alexander Hagenah, Head of Cyber Controls at SIX. It streamlines the process of identifying exploits for known vulnerabilities as well as the risk scoring of their respective exploitation probabilities.

Sources:

Directive - 2022/2555 - EN - EUR-Lex	**Final Text of the European Union's Network and Information Systems Security Directive 2 (NIS2)**
Regulation - 2022/2554 - EN - DORA - EUR-Lex	**Final Text of the EU's Digital Operational Resilience Act (EU DORA)**
Act relating to national security (Security Act) - Lovdata (ENG) Lov om nasjonal sikkerhet (sikkerhetsloven) - Lovdata (NOR)	**The Norwegian National Security Act**
SS1/21 Operational resilience: Impact tolerances for important business services | Bank of England	**The UK Prudential Regulatory Authority's Supervisory Statement 1/21 (PRA SS1/21)**
https://www.sec.gov/newsroom/press-releases/2023-227	**SEC press release on the SolarWinds cyber deficiencies identified in the complaint and charge.**
Cybersecurity Alerts & Advisories | CISA MITRE Corporation's New CVE ID Program on X CVEDETAILS.com powered by SecurityScoreCard	**Common Vulnerabilities & Exploits (CVE) databases (Images on Slide 5)**
Slides prepared by Chika Okoli, GRC Consultant & Forum Initiator: https://www.linkedin.com/in/chika-o-n/	