FULLHUNT
Expose your Attack Surface

SWISS CYBER STORM · 2026

Shadow IT

Mapping Switzerland's external attack surface

Mazin Ahmed
CTO & Founder, FullHunt · mazin@fullhunt.io

Shadow IT:
Exploiting External Attack Surface

Happy to Be Back

SWISS CYBER STORM · 16 OCTOBER 2016

2016

My first talk at Swiss Cyber Storm when I was 19.

2026

Today.

About Me

Mazin Ahmed

- **AppSec and Offensive Security Engineer**
- **Founder of FullHunt.io**
- **Occasional Bug Bounty Hunter: Acknowledged by Meta, X (formerly Twitter), LinkedIn, U.S. Department of Defense, and more**
- **In love 💛 with Cloud security, security automation, DevSecOps, distributed systems, and Web-App security**

FULLHUNT
Expose your Attack Surface

I have contributed to the security of the following:

And many more.

FULLHUNT
Expose your Attack Surface

My Recent Security Research

December 6, 2025

March 22, 2026

Follow mazinahmed.net/blog and fullhunt.io/blog for more.

What is Shadow IT?

If you don’t know every Internet-facing asset you have, you can’t secure them.

Types of shadow IT

Unauthorised Software

SaaS

Personal Devices

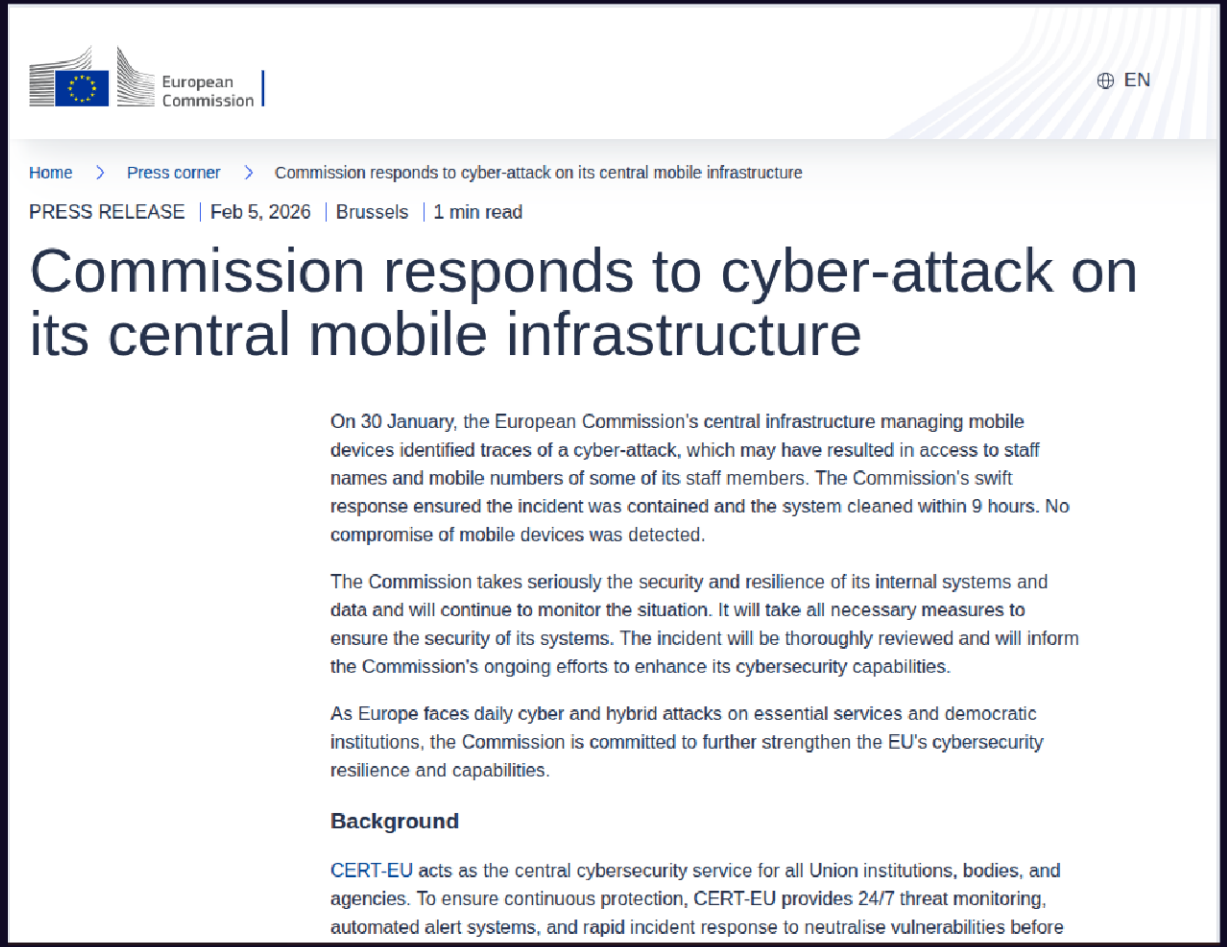
Undocumented Deployments

Untracked Employee Tools

Shadow Infrastructure

Forgotten cloud, staging and vendor assets facing the public internet.

This talk focuses on shadow infrastructure.



European Commission

EN

Home > Press corner > Commission responds to cyber-attack on its central mobile infrastructure

PRESS RELEASE | Feb 5, 2026 | Brussels | 1 min read

Commission responds to cyber-attack on its central mobile infrastructure

On 30 January, the European Commission's central infrastructure managing mobile devices identified traces of a cyber-attack, which may have resulted in access to staff names and mobile numbers of some of its staff members. The Commission's swift response ensured the incident was contained and the system cleaned within 9 hours. No compromise of mobile devices was detected.

The Commission takes seriously the security and resilience of its internal systems and data and will continue to monitor the situation. It will take all necessary measures to ensure the security of its systems. The incident will be thoroughly reviewed and will inform the Commission's ongoing efforts to enhance its cybersecurity capabilities.

As Europe faces daily cyber and hybrid attacks on essential services and democratic institutions, the Commission is committed to further strengthen the EU's cybersecurity resilience and capabilities.

Background

CERT-EU acts as the central cybersecurity service for all Union institutions, bodies, and agencies. To ensure continuous protection, CERT-EU provides 24/7 threat monitoring, automated alert systems, and rapid incident response to neutralise vulnerabilities before

HELP NET SECURITY

News Features CISO AI Videos Product showcase Industry news Reviews Whitepapers Events Newsletters

Zeljka Zorz, Editor-in-Chief, Help Net Security
February 9, 2026

European Commission hit by cyberattackers targeting mobile management platform

The European Commission's mobile device management platform was hacked but the incident was swiftly contained and no compromise of mobile devices was detected, EU's executive branch announced on Friday.

The intrusion was detected on January 30, 2026, by CERT-EU, the cybersecurity team protecting all European Union institutions, bodies, and agencies.

"The Commission's swift response ensured the incident was contained and the system cleaned within 9 hours," the EC stated, and added that the intrusion "may have resulted in access to staff names and mobile numbers of some of its staff members."

The Commission did not name the affected mobile device management platform, but it's widely speculated that it was Ivanti Endpoint Manager Mobile (EPMM), because the Dutch Data Protection Authority (AP) and the Council for the Judiciary (Rvdr) have recently suffered a data breach stemming from that platform's compromise.

Arno Rutte, the State Secretary for Justice and Security, informed the Dutch Parliament on Friday that those institutions' systems were recently hit by attackers.

"The National Cyber Security Centre (NCSC) was informed by the vendor on January 29th of vulnerabilities in EPMM. EPMM is used to manage mobile devices, apps, and content, including their security," Rutte stated in a letter to the Parliament.

"Based on the information currently available, I can report that at least the AP and the Rvdr have been affected. It has

EQUIFAX | INVESTOR RELATIONS

Press Releases

Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes

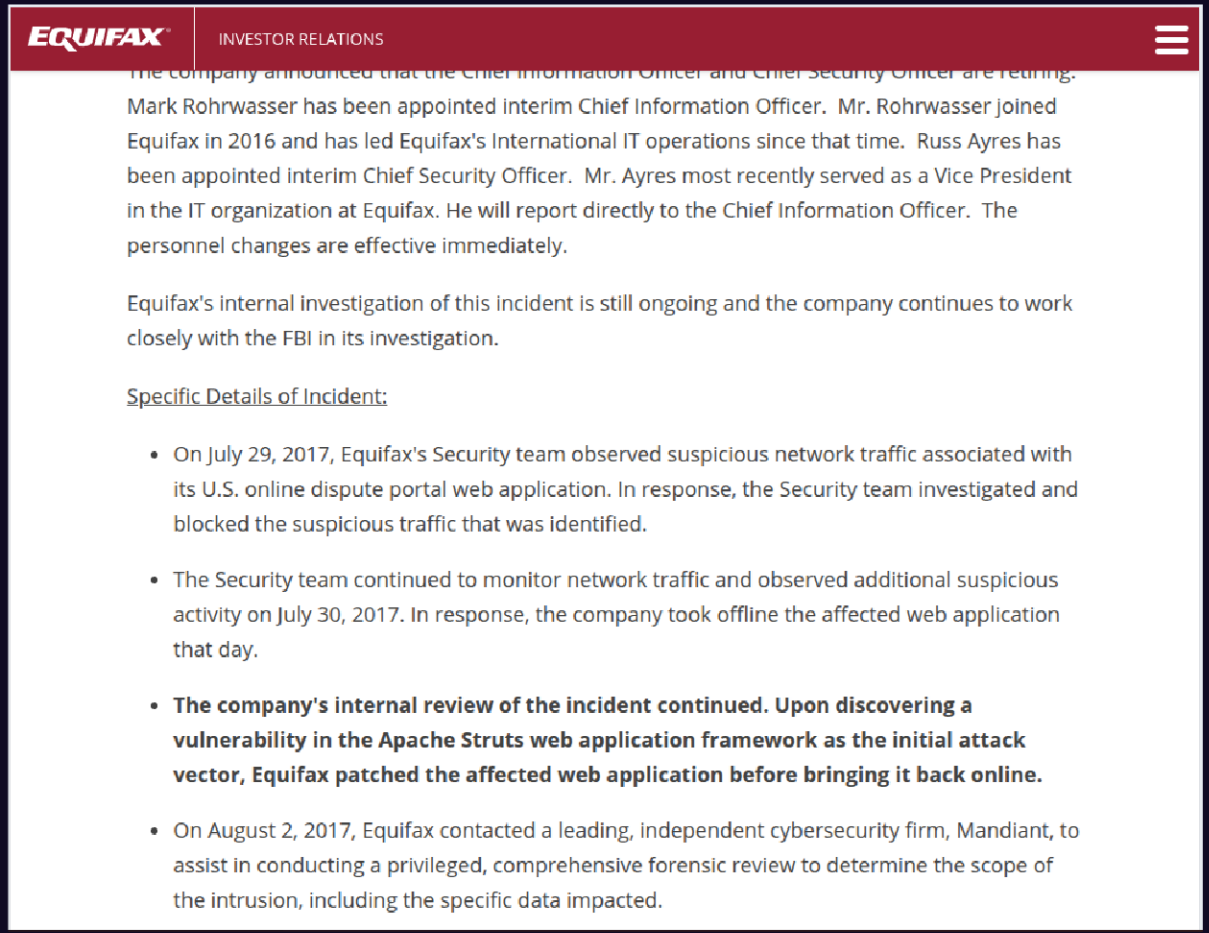
September 15, 2017 5:40pm EDT

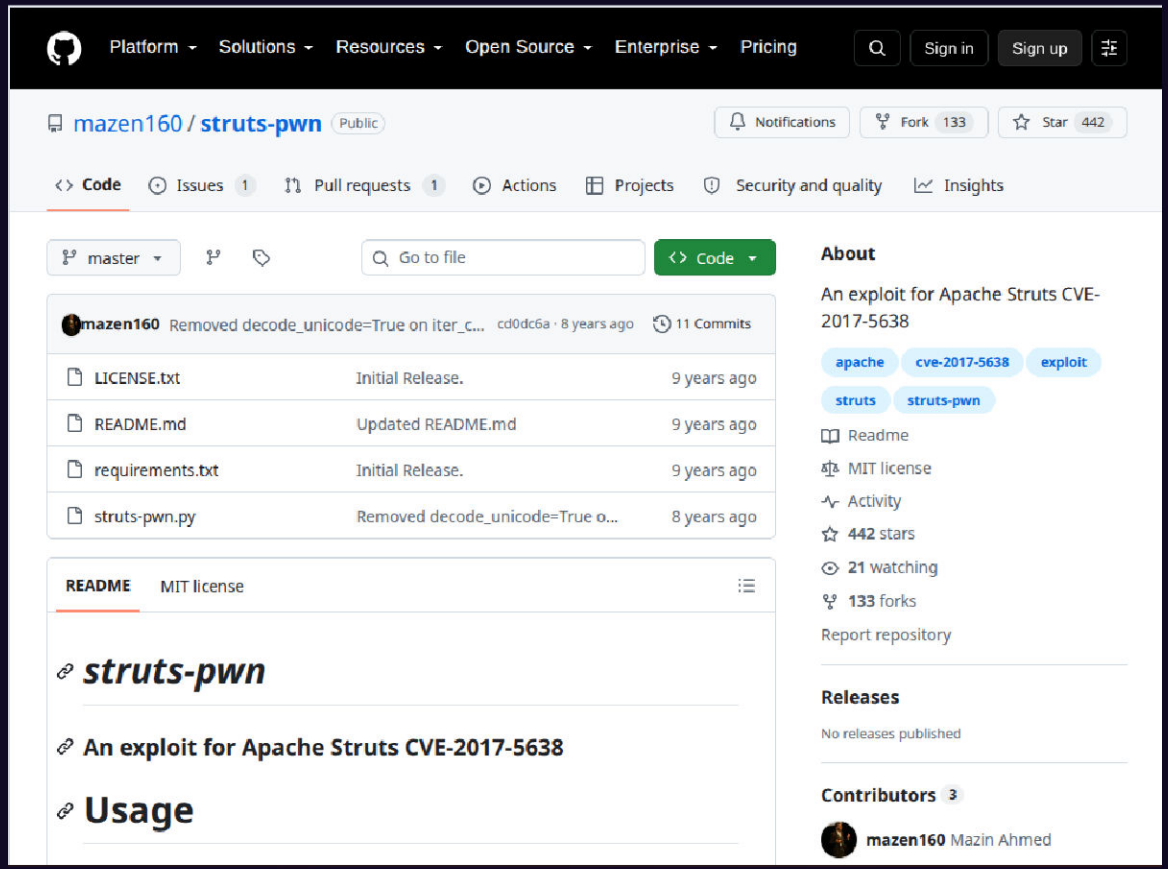
Download as PDF

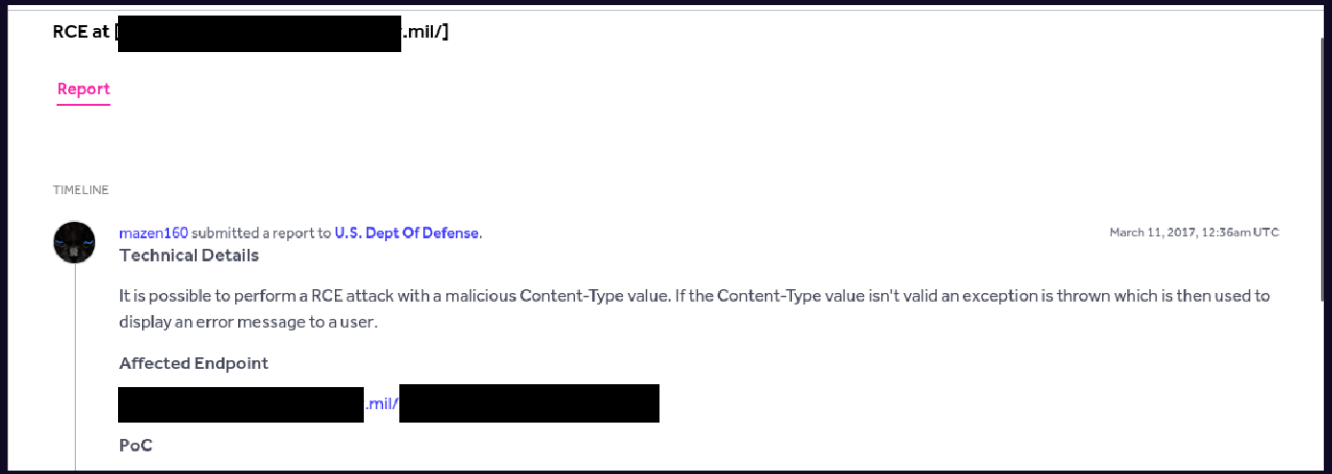
ATLANTA, Sept. 15, 2017 /PRNewswire/ -- As part of the company's ongoing review of the cybersecurity incident announced September 7, 2017, Equifax Inc. (NYSE: EFX) today made personnel changes and released additional information regarding its preliminary findings about the incident.

EQUIFAX®

The company announced that the Chief Information Officer and Chief Security Officer are retiring. Mark Rohrwasser has been appointed interim Chief Information Officer. Mr. Rohrwasser joined Equifax in 2016 and has led Equifax's International IT operations since that time. Russ Ayres has been appointed interim Chief Security Officer. Mr. Ayres most recently served as a Vice President in the IT organization at Equifax. He will report directly to the Chief Information Officer. The


EQUIFAX
INVESTOR RELATIONS
The company announced that the Chief Information Officer and Chief Security Officer are retiring. Mark Rohrwasser has been appointed interim Chief Information Officer. Mr. Rohrwasser joined Equifax in 2016 and has led Equifax's International IT operations since that time. Russ Ayres has been appointed interim Chief Security Officer. Mr. Ayres most recently served as a Vice President in the IT organization at Equifax. He will report directly to the Chief Information Officer. The personnel changes are effective immediately.
Equifax's internal investigation of this incident is still ongoing and the company continues to work closely with the FBI in its investigation.
Specific Details of Incident:
• On July 29, 2017, Equifax's Security team observed suspicious network traffic associated with its U.S. online dispute portal web application. In response, the Security team investigated and blocked the suspicious traffic that was identified.
• The Security team continued to monitor network traffic and observed additional suspicious activity on July 30, 2017. In response, the company took offline the affected web application that day.
• The company's internal review of the incident continued. Upon discovering a vulnerability in the Apache Struts web application framework as the initial attack vector, Equifax patched the affected web application before bringing it back online.
• On August 2, 2017, Equifax contacted a leading, independent cybersecurity firm, Mandiant, to assist in conducting a privileged, comprehensive forensic review to determine the scope of the intrusion, including the specific data impacted.


Platform
Solutions
Resources
Open Source
Enterprise
Pricing
Sign in
Sign up
mazen160 / struts-pwn
Public
Notifications
Fork 133
Star 442
Code
Issues 1
Pull requests 1
Actions
Projects
Security and quality
Insights
master
Go to file
Code
mazen160 Removed decode_unicode=True on iter_c... cd0dc6a · 8 years ago
11 Commits
LICENSE.txt Initial Release. 9 years ago
README.md Updated README.md 9 years ago
requirements.txt Initial Release. 9 years ago
struts-pwn.py Removed decode_unicode=True o... 8 years ago
README
MIT license
struts-pwn
An exploit for Apache Struts CVE-2017-5638
Usage
About
An exploit for Apache Struts CVE-2017-5638
apache
cve-2017-5638
exploit
struts
struts-pwn
Readme
MIT license
Activity
442 stars
21 watching
133 forks
Report repository
Releases
No releases published
Contributors 3
mazen160 Mazin Ahmed



RCE at [.mil/]

Report

TIMELINE

mazen160 submitted a report to U.S. Dept Of Defense. March 11, 2017, 12:36am UTC

Technical Details

It is possible to perform a RCE attack with a malicious Content-Type value. If the Content-Type value isn't valid an exception is thrown which is then used to display an error message to a user.

Affected Endpoint

.mil/

PoC

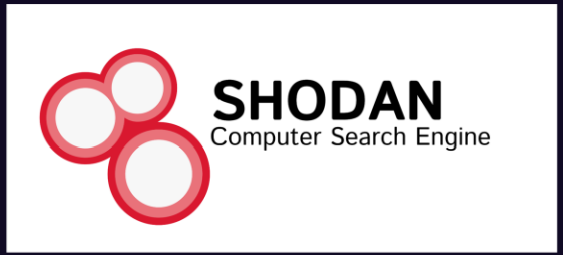
Why threat attackers target Shadow IT?

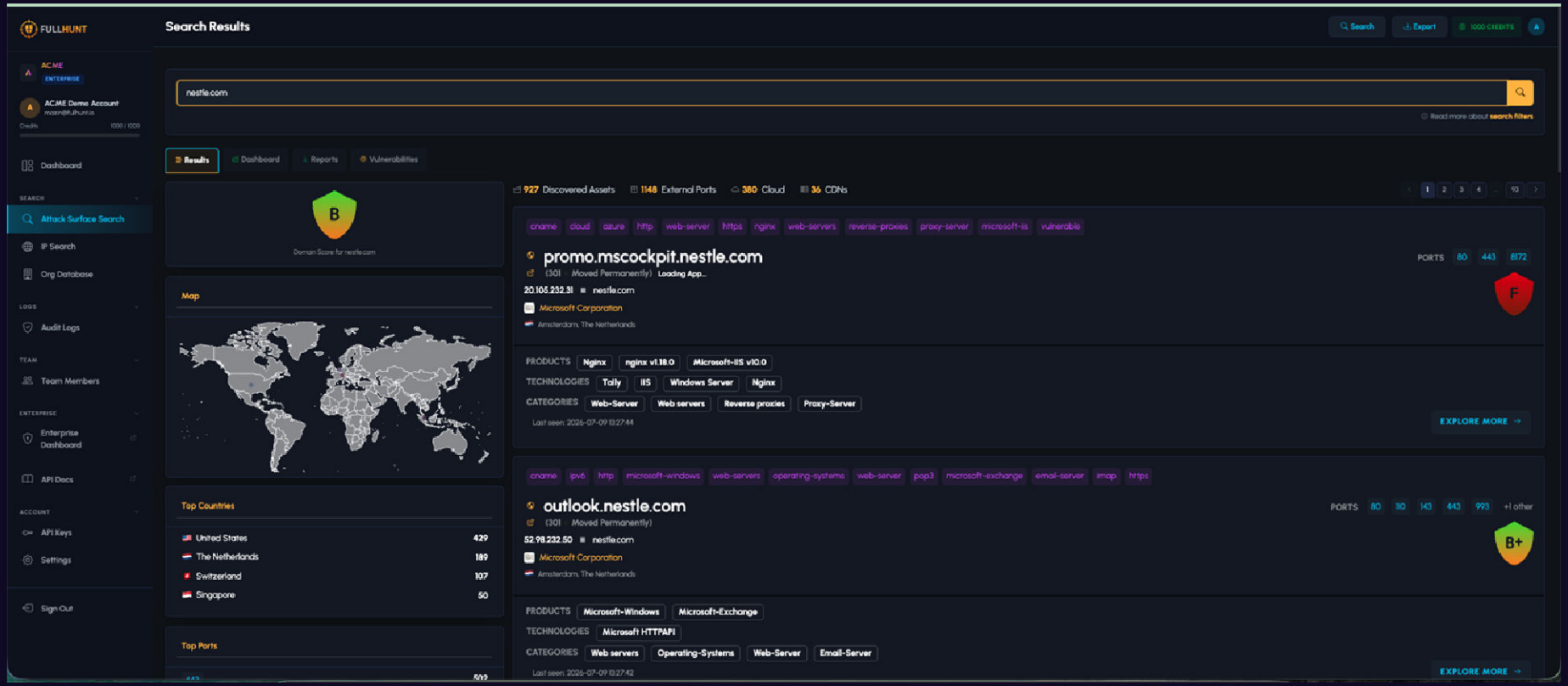
- Lower risk of detection.
- Lower risk in being caught.
- People are intelligent; it’s easier to attack IT assets.

How hackers expose attack surfaces

How attack surfaces are enumerated, fingerprinted and attributed.

Open Search Engines




FULLHUNT
Search Results
Search
Export
1000 CREDITS
ACME
ENTERPRISE
ACME Demo Account
Credits
1000 / 1000
nestle.com
Read more about search filters
Dashboard
Results
Dashboard
Reports
Vulnerabilities
SEARCH
Attack Surface Search
IP Search
Org Database
LOGS
Audit Logs
TEAM
Team Members
ENTERPRISE
Enterprise Dashboard
API Docs
ACCOUNT
API Keys
Settings
Sign Out
B
Domain Score for nestle.com
927 Discovered Assets
1148 External Ports
380 Cloud
36 CDNs
Map
Top Countries
United States 429
The Netherlands 189
Switzerland 107
Singapore 50
Top Ports
443 502
cname cloud azure http web-server https nginx web-servers reverse-proxies proxy-server microsoft-iis vulnerable
promo.mscockpit.nestle.com
(301 Moved Permanently) Loading App...
20.105.232.31 nestle.com
Microsoft Corporation
Amsterdam, The Netherlands
PORTS 80 443 8172
F
PRODUCTS Nginx nginx v1.18.0 Microsoft-IIS v10.0
TECHNOLOGIES Tally IIS Windows Server Nginx
CATEGORIES Web-Server Web servers Reverse proxies Proxy-Server
Last seen: 2026-07-09 13:27:44
EXPLORE MORE
cname ipv6 http microsoft-windows web-servers operating-systems web-server pop3 microsoft-exchange email-server imap https
outlook.nestle.com
(301 Moved Permanently)
52.98.232.50 nestle.com
Microsoft Corporation
Amsterdam, The Netherlands
PORTS 80 110 143 443 993 +1 other
B+
PRODUCTS Microsoft-Windows Microsoft-Exchange
TECHNOLOGIES Microsoft HTTPAPI
CATEGORIES Web servers Operating-Systems Web-Server Email-Server
Last seen: 2026-07-09 13:27:42
EXPLORE MORE

Why shadow infrastructure appears in the first place?

- New servers being deployed without security reviews.
- No documentation or playbooks.
- Employees move between organizations.
- People move between teams.
- Experiments and personal projects made without reviews.
- Mergers and Acquisitions (M&A).
- 3rd Party Companies.

Shadow IT in Switzerland

Shadow IT in Switzerland

- **~25M** IP Addresses
- Organizations: We mapped more than **3,000 Swiss organizations**, all searchable through **FullHunt.io**
- We identified **hundreds** of vulnerabilities at scale within Switzerland.

Results

Security Exposures Across the Swiss Internet

Exposed MySQL DBs

- FullHunt found 10,855 unique IPs running MySQL in Switzerland.
- From orgs we scanned: 1,512 hosts have public open MySQL services.
- 120 honeypots were detected.
  - Creds: 102 root/(empty) + 16 test/test + 2 root/root.

Exposed Mongo DBs

- FullHunt found 2,916 MongoDB instances in Switzerland.
- From orgs we scanned: 8 hosts have public open MongoDB services.
- 13 Mongo DBs do not have authentication enabled.
    - 7 DBs are already compromised according to FullHunt research with ransom left on the database.

Exposed Mongo DBs

```
  All your data was backed up by us. You must pay 0.0060 bitcoin to
  bc1qt6kstjjdatqnxd3ksdcfv0jnhdjzndcnkx8zla or in 48 hours, your
data
  will be publicly disclosed and deleted. (for more information
visit
  https://is.gd/2mongodb) After payment send mail to
ak+1j3rk0@onionmail.org
  and we will provide a link for you to download your data.
  Your DATAID is: 1J3RK0
```

Exposed Modern Attack Surfaces

Exposed Docker Registries

Exposed Docker Registries

- FullHunt discovered 26 Docker registries that are exposed to the Internet and allow anonymous access.
- Based on our research, threat actors could gain access to 180 unique repositories hosting 1,900 image tags, and hosting 24GB of Docker images.
- Docker images have embedded additional secrets, including DB credentials.

Exposed Docker Registries

- Deployments are pinned to specific image tags.
- An attacker can pull an image -> backdoor the build -> upload the build to the registry.
- Downstream systems could then pull the compromised image.

Exposed Docker Registries

A Docker Registry used by customers could be abused to become a supply-chain attack vector.

Exposed ElasticSearch Instances

Exposed ElasticSearch Instances

- FullHunt identified 1,970 ElasticSearch Instances in Switzerland.
- There are 76 instances that are accessible without authentication.
- Some instances belonged to large Swiss organizations and exposed Security Operations infrastructure data.

Exposed AI Gateways

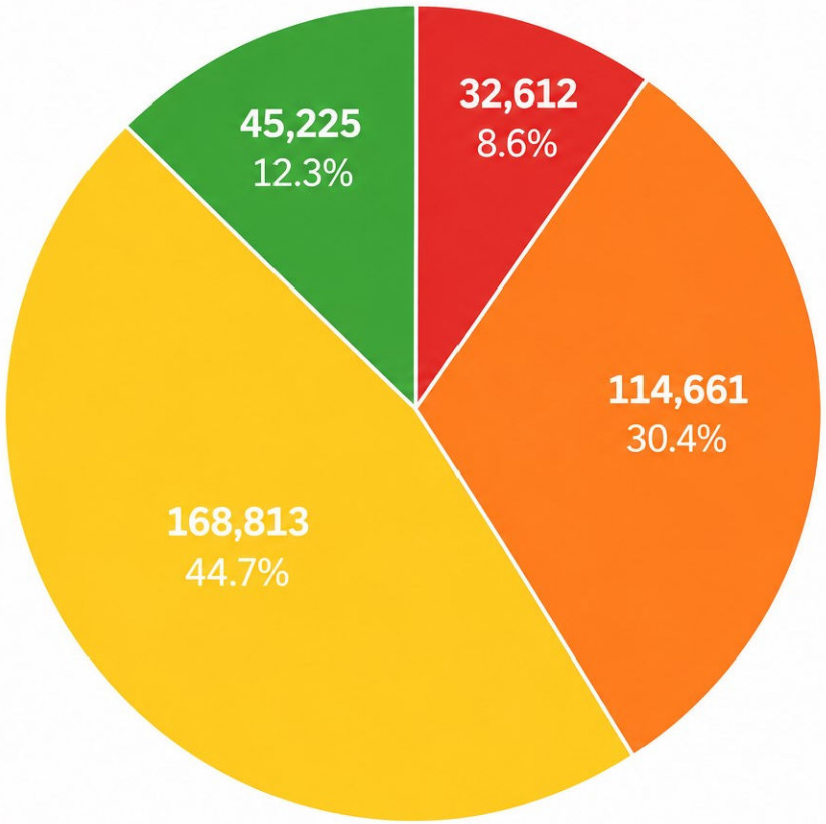
Exposed AI Gateways

- FullHunt identified 152 Ollama AI Gateways that exposed to the Internet.
- Threat actors can abuse these AI Gateways to use AI models on Swiss infrastructure for free.
- If there are proprietary models exposed on these AI gateways, threat actors would be able to pull these models.

Systems with Outdated Software

Passive FullHunt scanning revealed that at least 52% orgs scanned had systems with known vulnerabilities.

Vulnerabilities by Severity



- **Critical** 32,612 (8.6%)
- **High** 114,661 (30.4%)
- **Medium** 168,813 (44.7%)
- **Low** 45,225 (12.3%)

Honourable Mentions

- **Subdomain Takeover** vulnerabilities affecting more **66 Swiss Orgs**.
- **InfluxDB with no auth enabled for major Swiss companies**
- **CouchDB with no auth enabled** for **major Swiss companies**.
- Hundred of **Honeypots** were **easily discoverable**.

Reducing the surface:
Attack Surface Reduction Framework

What national CERTs can do

Swiss NCSC

- Swiss NCSC runs external Internet scans, but results are not shard.
- Switzerland's external attack surface security is mature overall, but a broader coverage is still needed.

Vulnerability research is important

- First Security Technology used to publish an annual report on Switzerland's external vulnerability landscape.
- The company has since shut down - and we need this kind of research now more than ever.

Vulnerability research is important

RiskioMonitor, an Austrian company, published a Shadow IT report analyzing Swiss domains, with a particular focus on dark web exposure and data breaches.

RECOMMENDATIONS

What national CERTs can do

Continuous Vulnerability Research

Continuous Internet-wide scans on the nation's attack surface

Index all products running across all exposed assets on the nation's attack surface

Product attribution is difficult.

Takeaways

01 You cannot secure what you have not found.

02 Attackers optimise for gaps in process.

03 Country-scale visibility is achievable.

FULLHUNT
Expose your Attack Surface

QUESTIONS

Thank you

- mazin@fullhunt.io
- fullhunt.io
- @mazen160

EXPLORE YOUR ATTACK SURFACE AT FULLHUNT.IO