



Number One Risk: Not Knowing your Asset Inventory

Agenda

- Who am I
- Security Requirements
- Why is Asset Management Important
- Breaches Caused by Insufficient Asset Inventories
- Holistic Visibility of Attack Surface





Who Am I?

Aaron Sanderson

Senior Penetration Tester / Threat Analyst
CISSP, C|EH

Subject Matter Expert

- Penetration Testing
- Cyber Forensics
- Website Scanning and Exploitation Tools
- Vulnerability Scanning
- Incident Response and Reporting
- Network/Endpoint/Information Security
- Computer Network Defense

Red Team Operator/Penetration Tester/Threat Analyst

Navy Red Team (one of nine NSA Certified DoD Red Teams) providing on-board Cyber Threat Emulation during Fleet, Command, and Joint Exercises during pre-deployment training, acquisition program assessments, and operational readiness assessments.

Clearance

Active Top Secret/SCI with current SSBI

30 Years in IT

Focused on Security since 2004

Penetration Tester since 2018

Aarons@JanusAssociates.com

@SecurityAaron





Top Security Controls

CIS Critical Security Control 1: Inventory and Control of Enterprise Assets support identifying unauthorized and unmanaged assets to remove or remediate; and **CIS Critical Security Control 2: Inventory and Control of Software Assets** ensures authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution

The Payment Card Industry Data Security Standard (PCI DSS) requires that an inventory of system components (PCI Req. 2.4: Complete Inventory List) is maintained.

NIST 800-53 Revision 5 CM-8 System Component Inventory requires an organization to develop and document an inventory of system components, and review and update the system component inventory regularly

NIST Cybersecurity Framework ID.AM-1: Physical devices and systems within the organization are inventoried; **ID.AM-2:** Software platforms and applications within the organization are inventoried; and **ID.AM-4:** External information systems are catalogued

ISO 27001 A.8.1.1 Inventory of Assets: Any assets associated with information and information processing facilities need to be identified and managed over the lifecycle, always up to date



Why is Asset Management Important

Internet-accessible assets have grown exponentially increasing the attack surface

Malicious actors scan the Internet searching for vulnerabilities and/or weaknesses on assets that are not properly managed

Mismanaged assets become hard to track and determine what needs protection

Unknown assets can include Shadow IT, test and deployment servers, login portals, temporary services, etc.

Data leakage due to vulnerable and publicly accessible information systems hosting an internal system

Which Assets?

- Known
- 3rd Party
- Shadow IT
- Rogue



Shadow IT

- Companies or organizations may not know of information technology
- Employees are using information technology without company approval
- Shadow IT can be an application, cloud-based services, or hardware
- Examples of Shadow IT are unapproved communication and collaboration tools (Slack, Dropbox, WhatsApp, etc.)



Rogue Assets

- An unauthorized node on a network
- Can include a list of discovered assets not currently present in the asset inventory
- Can be hardware or software
- Best detection method is regular network discovery scans and/or vulnerability scanning across the network



Apache Struts

- CVE-2017-05638
- Published March 6
- Scanning started March 9
- Initial Breaches March 14

- Equifax was breached two months later

```
<Variable name="textColor" description="Text Color"
  type="color" default="#204063" value="#204063">
<Variable name="blogTitleColor" description="Blog Title Color"
  type="color" default="#eef6fe" value="#eef6fe">
<Variable name="blogDescriptionColor" description="Blog Description Color"
  type="color" default="#eef6fe" value="#eef6fe">
<Variable name="postTitleColor" description="Post Title Color"
  type="color" default="#477fba" value="#477fba">
<Variable name="dateHeaderColor" description="Date Header Color"
  type="color" default="#8facc8" value="#8facc8">
<Variable name="sidebarHeaderColor" description="Sidebar Title Color"
  type="color" default="#809fbd" value="#809fbd">
<Variable name="linkColor" description="Link Color"
  type="color" default="#309fbd" value="#309fbd">
<Variable name="visitedLinkColor" description="Visited Link Color"
  type="color" default="#4386ce" value="#4386ce">
<Variable name="sidebarLinkColor" description="Sidebar Link Color"
  type="color" default="#2462a5" value="#2462a5">
<Variable name="visitedSidebarLinkColor" description="Visited Sidebar Link Color"
  type="color" default="#599be2" value="#599be2">
<Variable name="visitedLinkColor" description="Visited Link Color"
  type="color" default="#3372b6" value="#3372b6">
```

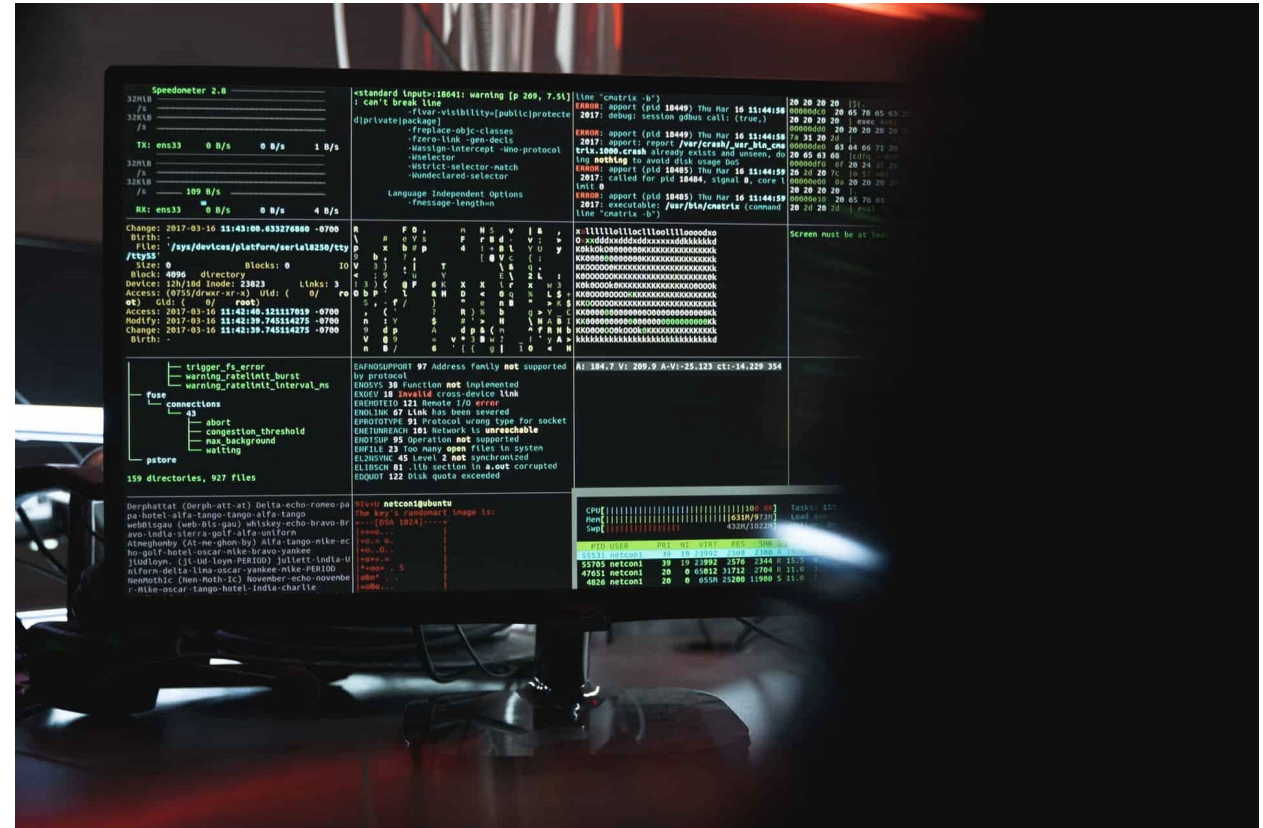
Other Breaches

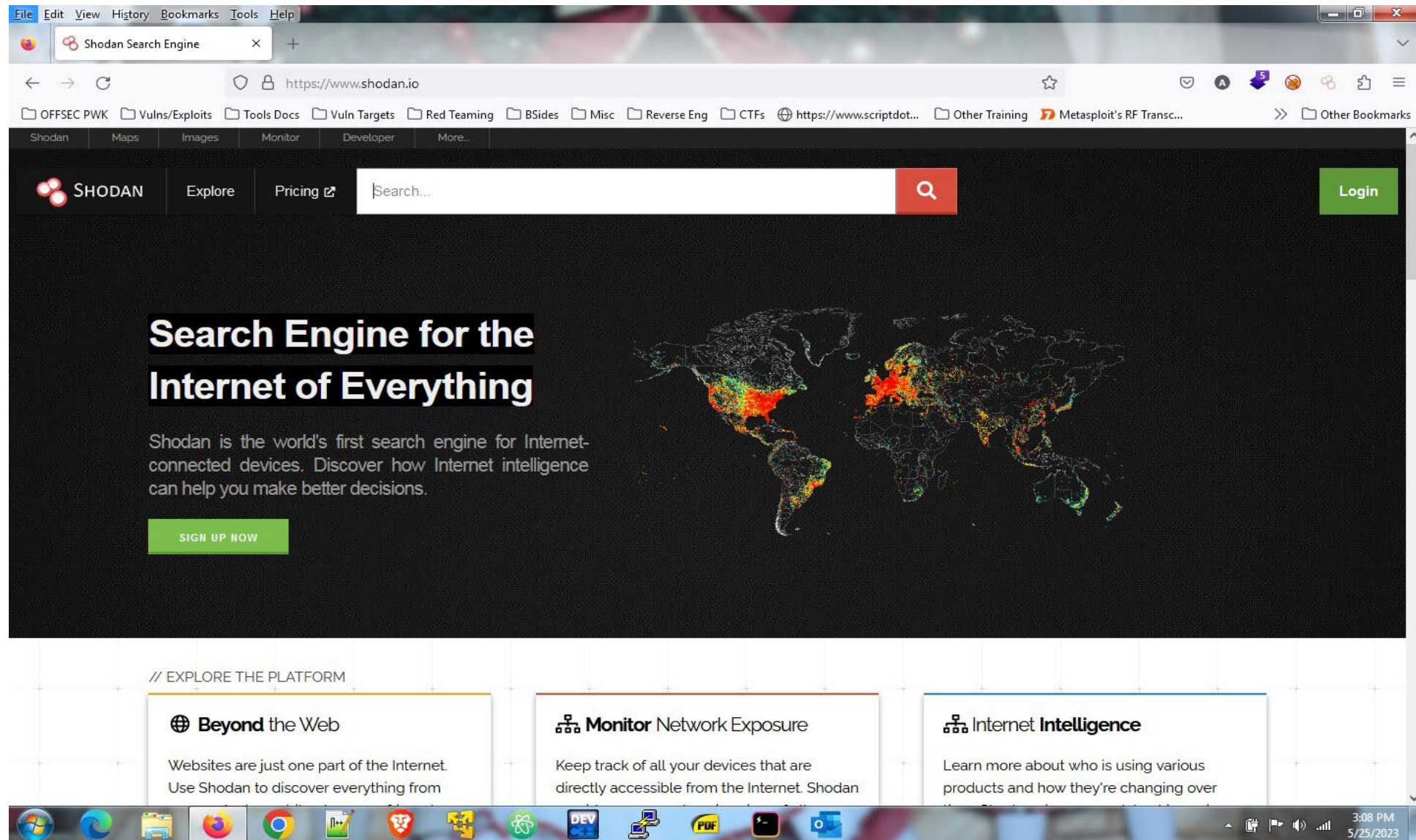
- **Target** (Unsegmented HVAC Controls. 40 million credit and debit card numbers and 70 million records of personal information were stolen)
- **OPM** (Shared Network Infrastructure with another Agency. PHI Breach = 22.1 million people)
- **WeWork** (Inputting WeWork name into Resonance platform resulted in source code & credentials. PII spill of over 40,000 data sets)
- **Global Big 4 Consulting Firm** (Leakage of PII, Client Names, Project Names, Partner Details, Storage System credentials including sheets and documents, System logs, and operations)



An Attacker's Visibility

- Shodan.io / Masscan
- Builtwith
- Wappalyzer





File Edit View History Bookmarks Tools Help

Shodan Search Engine

https://www.shodan.io

OFFSEC PWK Vulns/Exploits Tools Docs Vuln Targets Red Teaming BSides Misc Reverse Eng CTFs https://www.scriptdot... Other Training Metasploit's RF Transc... Other Bookmarks

Shodan Maps Images Monitor Developer More...

SHODAN Explore Pricing Search... Login

Search Engine for the Internet of Everything

Shodan is the world's first search engine for Internet-connected devices. Discover how Internet intelligence can help you make better decisions.

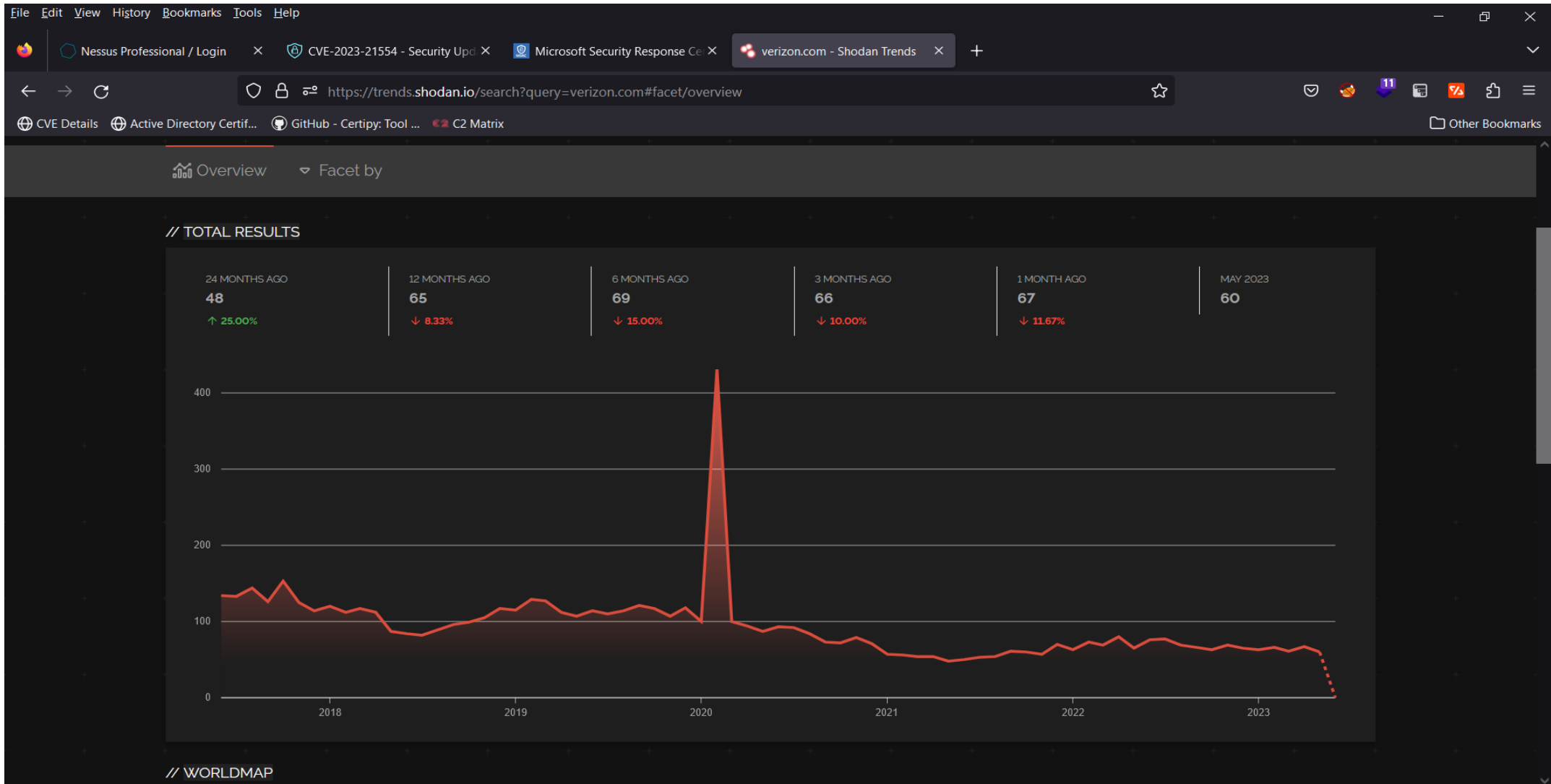
SIGN UP NOW

// EXPLORE THE PLATFORM

- Beyond the Web**
Websites are just one part of the Internet. Use Shodan to discover everything from
- Monitor Network Exposure**
Keep track of all your devices that are directly accessible from the Internet. Shodan
- Internet Intelligence**
Learn more about who is using various products and how they're changing over

3:08 PM 5/25/2023

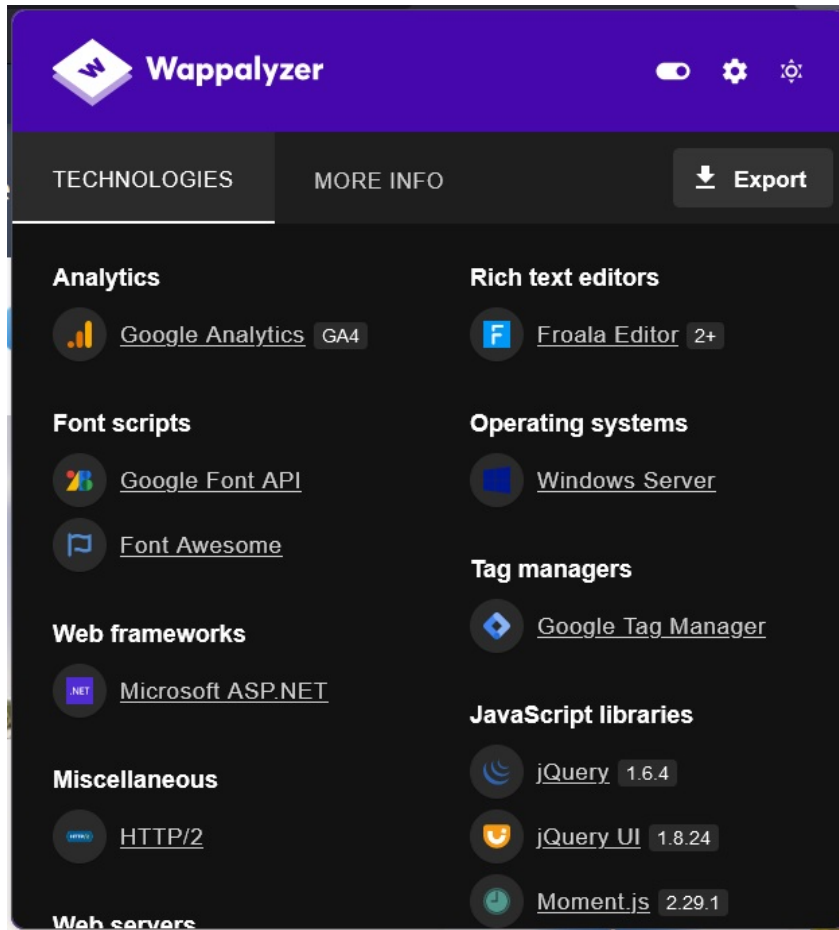
Shodan Historical Data





Builtwith

The screenshot shows a web browser window with the URL `builtwith.com`. The browser's tab bar contains several open tabs, including `attack s`, `sans at`, `This is a`, `SANS_T`, `Cyber S`, `New Tal`, `Comba`, `Module`, `URL an`, `BuiltWi`, `Azure B`, and `DigitalC`. The browser's address bar shows `builtwith.com`. The page's navigation bar is dark green and features the `builtwith` logo, a `Log In · Signup for Free` link, and a search bar with the text `Website, Tech, Keyword` and a `Lookup` button. The main content area has a large heading `Find out what websites are Built With` and a search input field with the placeholder text `Enter a website address, a technology name or a keyword` and a `Lookup` button. At the bottom of the page, there is a red button that says `Download Full Lead List` and a link to `Create a Free Account to see more results.`



Wappalyzer

TECHNOLOGIES | MORE INFO | Export

- Analytics**
 - Google Analytics GA4
- Font scripts**
 - Google Font API
 - Font Awesome
- Web frameworks**
 - Microsoft ASP.NET
- Miscellaneous**
 - HTTP/2
- Rich text editors**
 - Froala Editor 2+
- Operating systems**
 - Windows Server
- Tag managers**
 - Google Tag Manager
- JavaScript libraries**
 - jQuery 1.6.4
 - jQuery UI 1.8.24
 - Moment.js 2.29.1
- Web servers**

CVE Details

The ultimate security vulnerability datasource

[Log In](#) [Register](#) [Take a third party risk management course for FREE](#)

[Switch to https://](#)
[Home](#)

Browse :

- [Vendors](#)
- [Products](#)
- [Vulnerabilities By Date](#)
- [Vulnerabilities By Type](#)

Reports :

- [CVSS Score Report](#)
- [CVSS Score Distribution](#)

Search :

- [Vendor Search](#)
- [Product Search](#)
- [Version Search](#)
- [Vulnerability Search](#)
- [By Microsoft References](#)

Top 50 :

- [Vendors](#)
- [Vendor Cvss Scores](#)
- [Products](#)
- [Product Cvss Scores](#)
- [Versions](#)

Other :

Momentjs » Moment » **** : Security Vulnerabilities

Cpe Name: `cpe:2.3:a:momentjs:moment:*:*:*:*:*:node.js:*:*`

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gain
1	CVE-2022-31129	400			2022-07-06	2023-02-23	5.0	
moment is a JavaScript date library for parsing, validating, manipulating, and formatting dates. Affected versions of moment parsing in moment (more specifically rfc2822 parsing, which is tried by default) has quadratic (N^2) complexity on specific input characters. Users who pass user-provided strings without sanity length checks to moment constructor are vulnerable to (Re versions with minimal tweaking. Users are advised to upgrade. Users unable to upgrade should consider limiting date lengths								
2	CVE-2022-24785	22		Dir. Trav.	2022-04-04	2023-02-16	5.0	
Moment.js is a JavaScript date library for parsing, validating, manipulating, and formatting dates. A path traversal vulnerability especially if a user-provided locale string is directly used to switch moment locale. This problem is patched in 2.29.2, and the provided locale name before passing it to Moment.js.								
3	CVE-2017-18214	400		DoS	2018-03-04	2022-02-14	5.0	
The moment module before 2.19.3 for Node.js is prone to a regular expression denial of service via a crafted date string, a c								
4	CVE-2016-4055	400		DoS	2017-01-23	2022-06-06	7.8	
The duration function in the moment package before 2.11.2 for Node.js allows remote attackers to cause a denial of service								



We are JANUS Associates

Trusted NYS Information Security Consultants

- Vendor-neutral, Cyber security specialists
- Founded 1988, the longest continuously operating IT Security specialty consultancy in US.
- Industry Certified, Senior Level Subject Matter Experts – only
- 34+ years serving government, business, and non-profits
- Privately held, WBE (woman-owned business)
- GSA Multiple Award Schedule (MAS) Contract: GS-35F-471BA
- **NYS PBITS Contract #PB028AA**

JANUS Corporate Headquarters

2 Omega Drive
Stamford, CT 06907
(203) 251-0200
www.janusassociates.com

Aaron Sanderson CISSP, CEH, Sr. Penetration Tester
Aarons@janusassociates.com
O: (203) 251-0222
C: (503) 780-8268

Philip Massa, Director
phillipm@janusassociates.com
O:(203) 251-0234
C: (203) 999-3324

