Kwetsbaarheden en Business Risico: ‘Hoe bepaal ik het verschil in mijn IT/OT landschap?’

Jerry Zwanenburg, Sr. Security Engineer

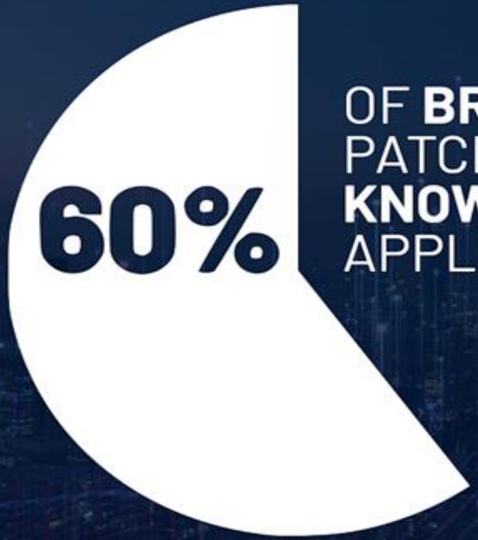
Date: 28.10.2020

tenable

1/2 OF THE MOST **COMMON VULNERABILITIES USED IN TARGETED ATTACKS AND TO DELIVER MALWARE** ARE MORE THAN A YEAR OLD

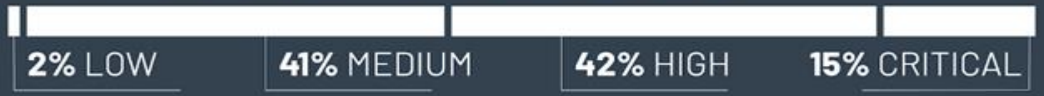
“NSA HAS **NOT RESPONDED TO AN INTRUSION USING A 0-DAY** EXPLOIT IN THE LAST 24 MONTHS”

David Hogue
Technical Director, NSA



OF **BREACHES OCCUR** BECAUSE A PATCH WAS AVAILABLE FOR A **KNOWN VULNERABILITY** BUT NOT APPLIED

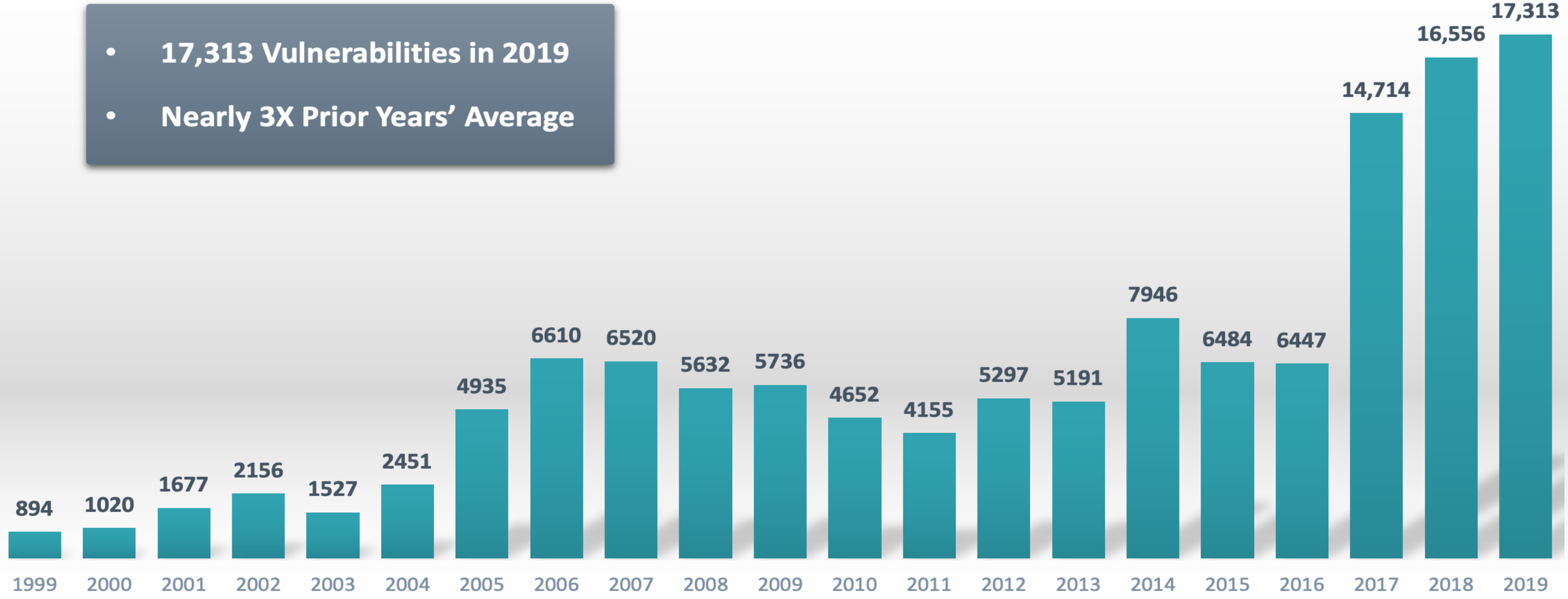
17K VULNERABILITIES DISCLOSED IN 2019



tenable

The Number of New Vulnerabilities Continues to Grow

- **17,313 Vulnerabilities in 2019**
- **Nearly 3X Prior Years' Average**



Source: Vulnerability Intelligence Report, Tenable Research

tenable

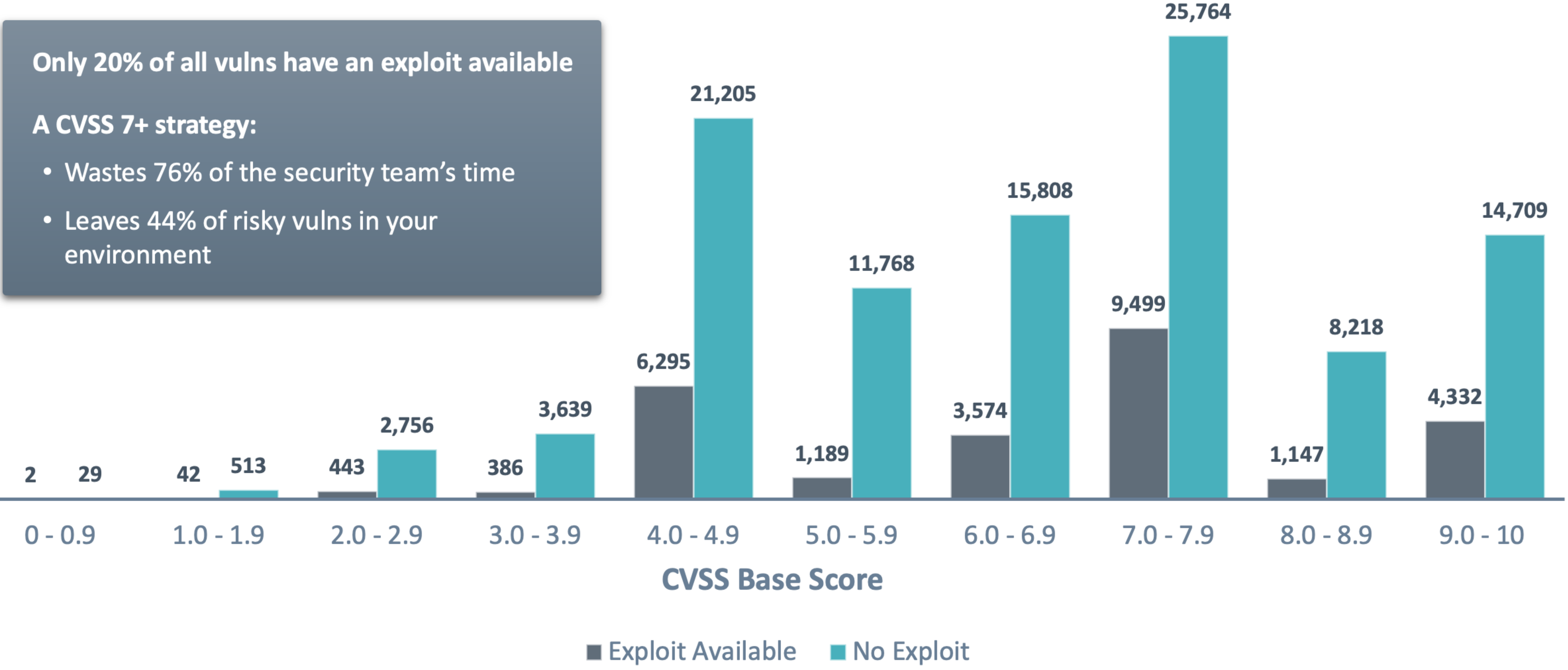
Source: Vulnerability Intelligence Report, Tenable Research

CVSS is a Poor Indicator of Risk

Only 20% of all vulns have an exploit available

A CVSS 7+ strategy:

- Wastes 76% of the security team's time
- Leaves 44% of risky vulns in your environment



When business leaders ask

"HOW SECURE ARE WE?"

They don't want a 300 page answer

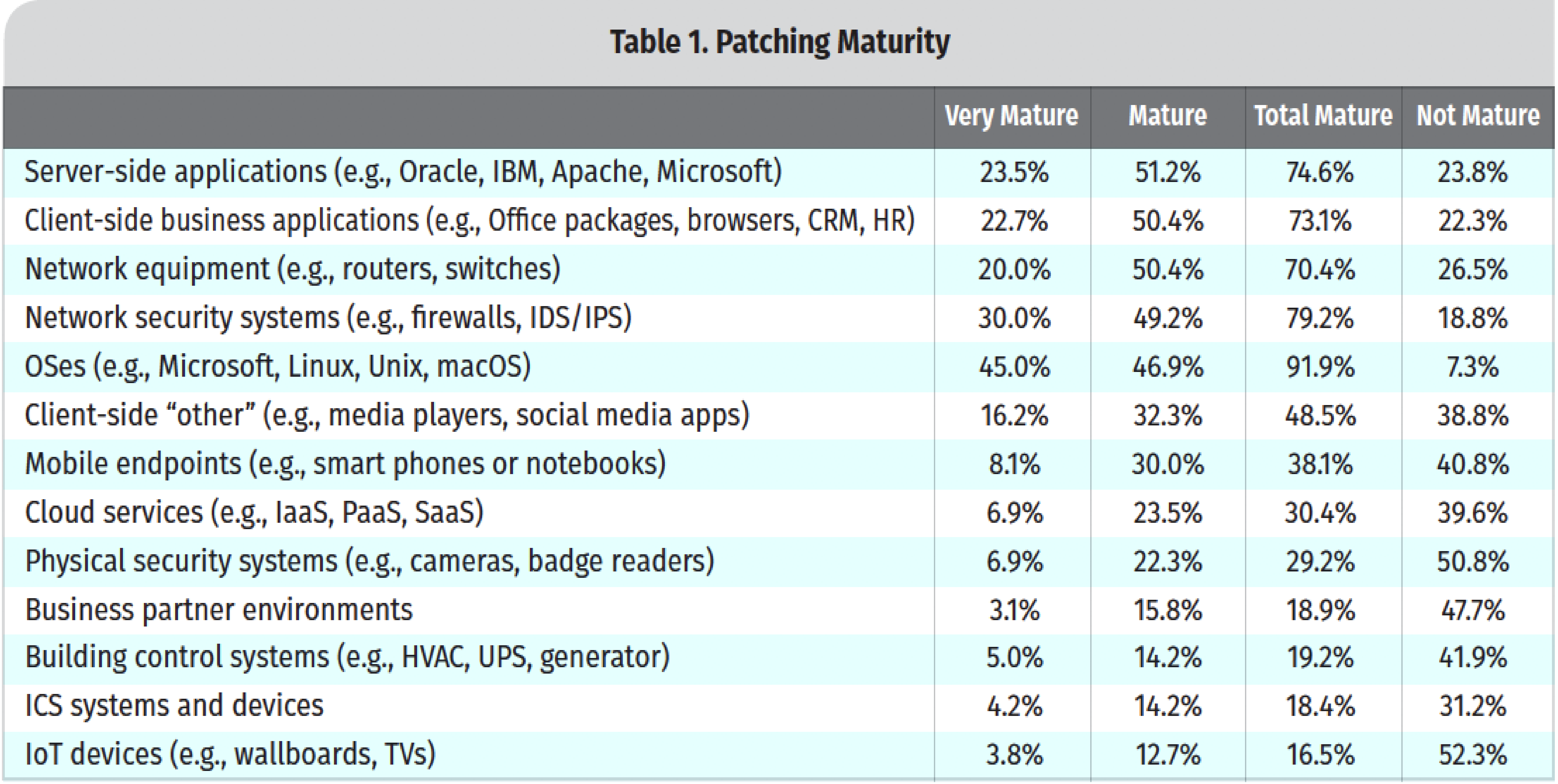
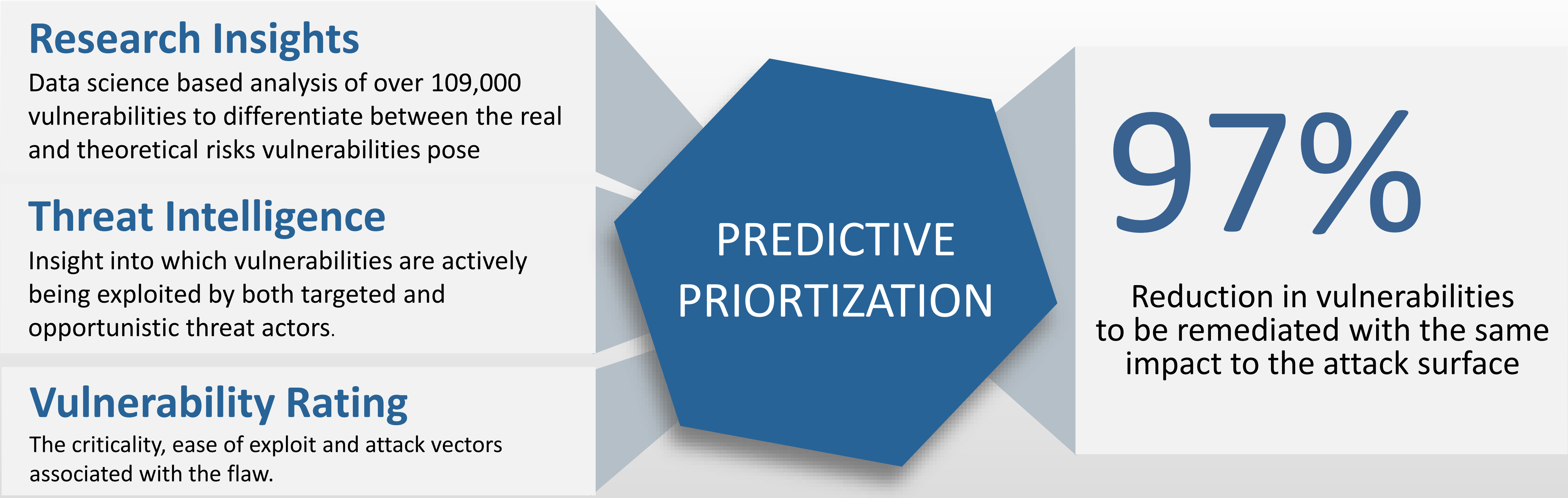


Table 1. Patching Maturity

	Very Mature	Mature	Total Mature	Not Mature
Server-side applications (e.g., Oracle, IBM, Apache, Microsoft)	23.5%	51.2%	74.6%	23.8%
Client-side business applications (e.g., Office packages, browsers, CRM, HR)	22.7%	50.4%	73.1%	22.3%
Network equipment (e.g., routers, switches)	20.0%	50.4%	70.4%	26.5%
Network security systems (e.g., firewalls, IDS/IPS)	30.0%	49.2%	79.2%	18.8%
OSes (e.g., Microsoft, Linux, Unix, macOS)	45.0%	46.9%	91.9%	7.3%
Client-side “other” (e.g., media players, social media apps)	16.2%	32.3%	48.5%	38.8%
Mobile endpoints (e.g., smart phones or notebooks)	8.1%	30.0%	38.1%	40.8%
Cloud services (e.g., IaaS, PaaS, SaaS)	6.9%	23.5%	30.4%	39.6%
Physical security systems (e.g., cameras, badge readers)	6.9%	22.3%	29.2%	50.8%
Business partner environments	3.1%	15.8%	18.9%	47.7%
Building control systems (e.g., HVAC, UPS, generator)	5.0%	14.2%	19.2%	41.9%
ICS systems and devices	4.2%	14.2%	18.4%	31.2%
IoT devices (e.g., wallboards, TVs)	3.8%	12.7%	16.5%	52.3%

Source 2019 SANS Vulnerability Management Survey Report

Vulnerability Priority Rating



Research Insights

Data science based analysis of over 109,000 vulnerabilities to differentiate between the real and theoretical risks vulnerabilities pose

Threat Intelligence

Insight into which vulnerabilities are actively being exploited by both targeted and opportunistic threat actors.

Vulnerability Rating

The criticality, ease of exploit and attack vectors associated with the flaw.

PREDICTIVE PRIORTIZATION

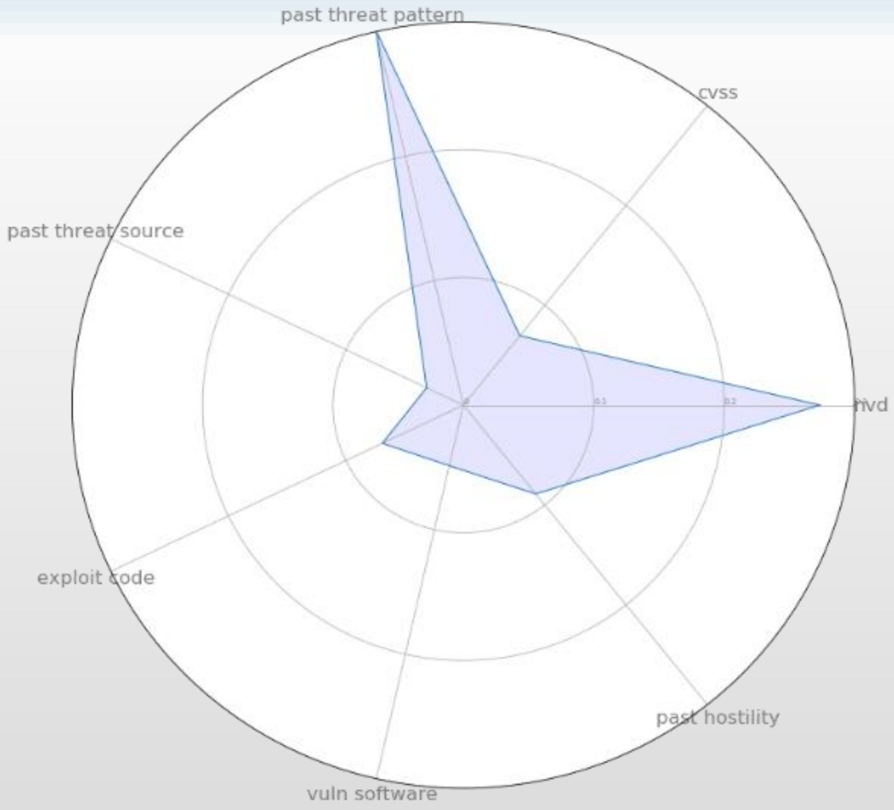
97%

Reduction in vulnerabilities to be remediated with the same impact to the attack surface

A Data Science Approach: Understanding the Model

150 different aspects in 7 groupings

- Past threat pattern
- CVSS
- NVD
- Past hostility
- Vulnerable software
- Exploit code
- Past threat source



Over **109,000** vulnerabilities tracked

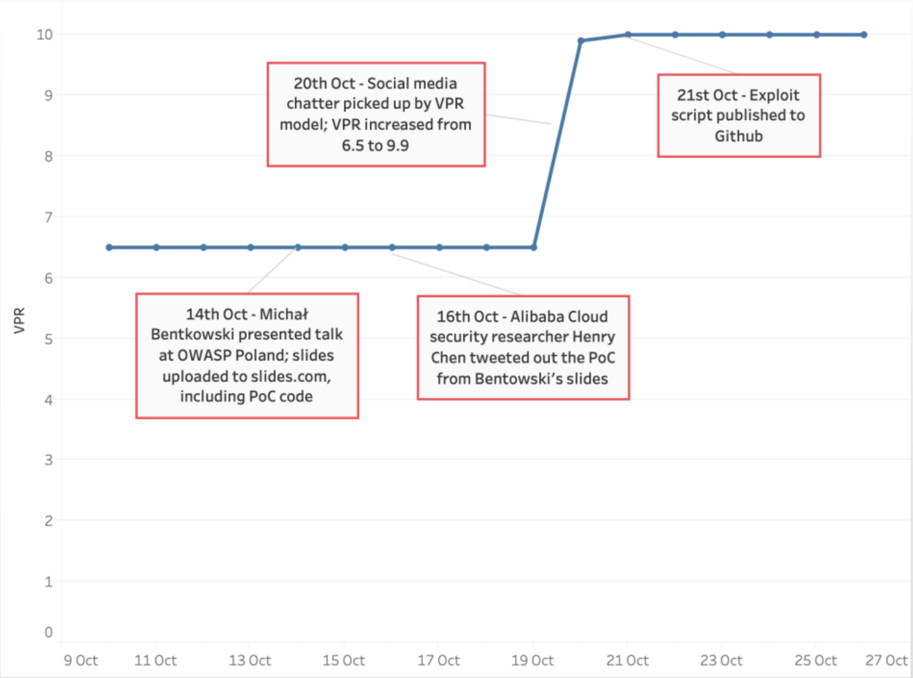
Forecasts probability of exploit in near term future

Dynamic Scoring Reflects Threat Environment

Example VPR

CVE-2019-7609

On October 21, an exploit script was published to GitHub for a patched vulnerability in Kibana, the open-source data visualization plugin for Elasticsearch. Elasticsearch and Kibana are part of the popular Elastic Stack (also known as ELK Stack), a series of open-source applications used for centralized log management.



20th Oct - Social media chatter picked up by VPR model; VPR increased from 6.5 to 9.9

21st Oct - Exploit script published to Github

14th Oct - Michał Bentkowski presented talk at OWASP Poland; slides uploaded to slides.com, including PoC code

16th Oct - Alibaba Cloud security researcher Henry Chen tweeted out the PoC from Bentowski's slides

Vulnerability in Oracle Access Manager Component of Oracle Fusion Middleware

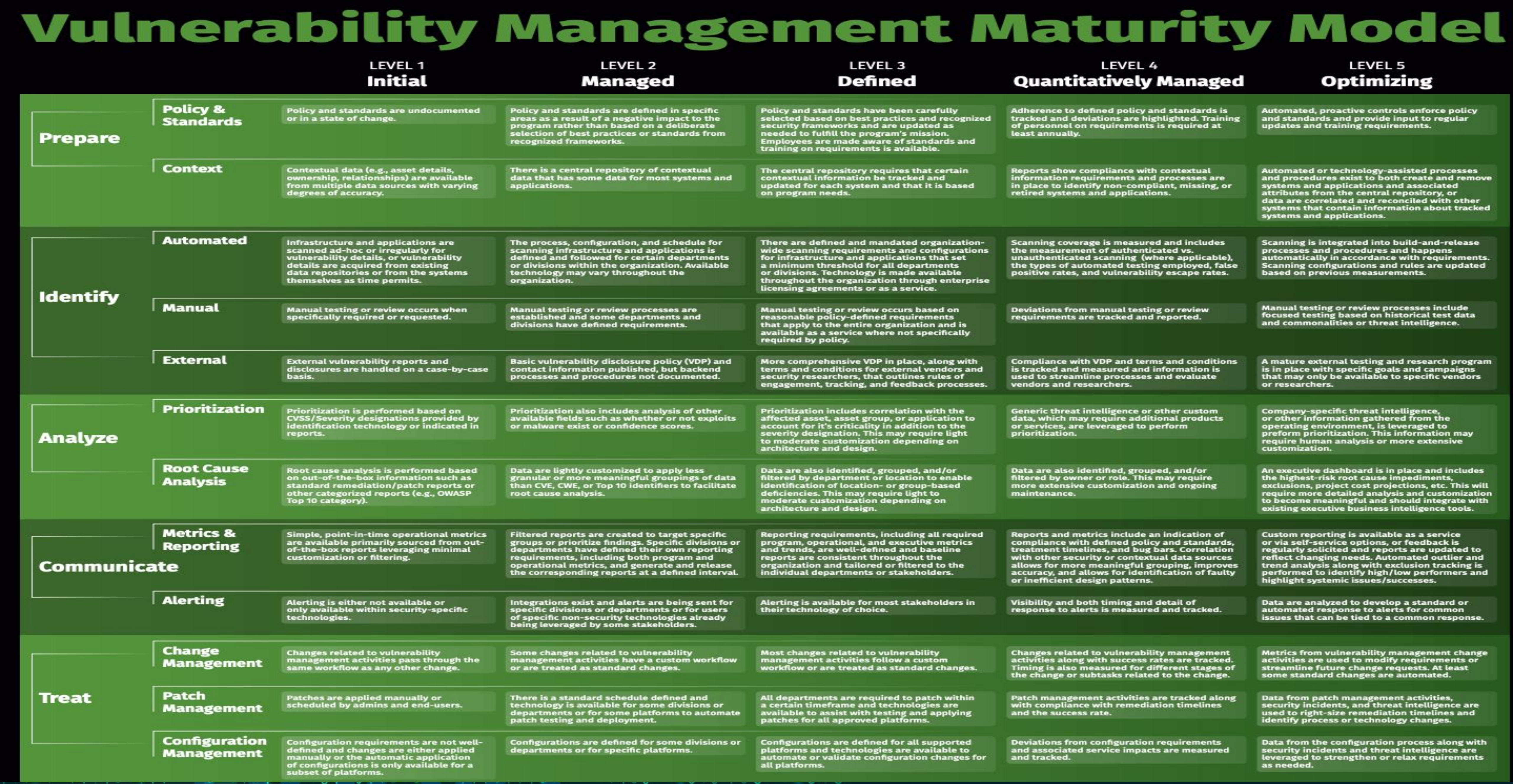
Vulnerability in Oracle Access Manager Component of Oracle Fusion Middleware

Waar begin ik

- https://www.sans.org/reading-room/whitepapers/projectmanagement/building-vulnerability-management-program-project-management-approach-35932

- https://static.tenable.com/marketing/whitepapers/Whitepaper-2019_SANS_Vulnerability_Management_Survey.pdf

- https://www.hackmageddon.com/category/security/cyber-attacks-statistics/

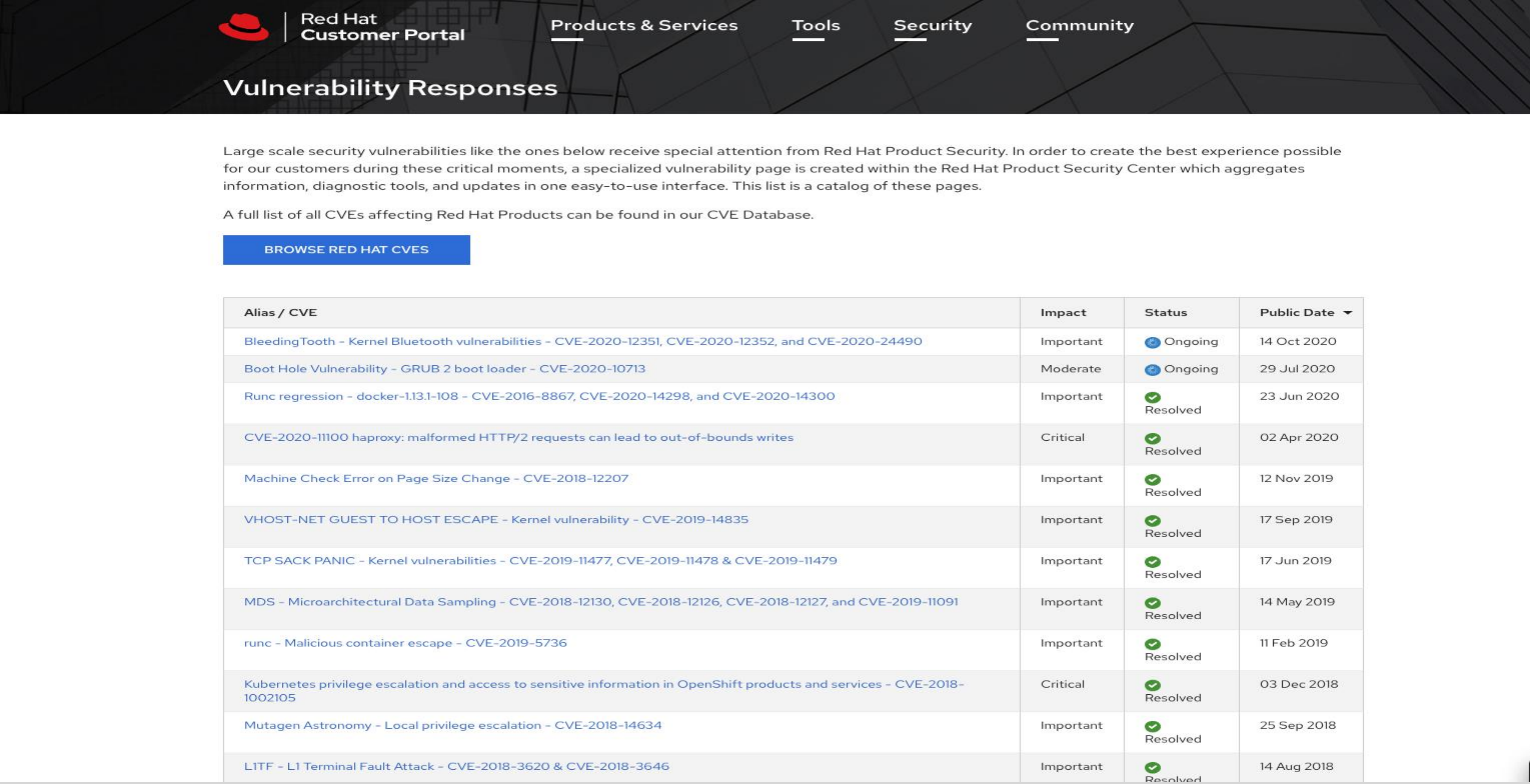


Vulnerability Management Maturity Model

		LEVEL 1 Initial	LEVEL 2 Managed	LEVEL 3 Defined	LEVEL 4 Quantitatively Managed	LEVEL 5 Optimizing
Prepare	Policy & Standards	Policy and standards are undocumented or in a state of change.	Policy and standards are defined in specific areas as a result of a negative impact to the program rather than based on a deliberate selection of best practices or standards from recognized frameworks.	Policy and standards have been carefully selected based on best practices and recognized security frameworks and are updated as needed to fulfill the program's mission. Employees are made aware of standards and training on requirements is available.	Adherence to defined policy and standards is tracked and deviations are highlighted. Training of personnel on requirements is required at least annually.	Automated, proactive controls enforce policy and standards and provide input to regular updates and training requirements.
	Context	Contextual data (e.g., asset details, ownership, relationships) are available from multiple data sources with varying degrees of accuracy.	There is a central repository of contextual data that has some data for most systems and applications.	The central repository requires that certain contextual information be tracked and updated for each system and that it is based on program needs.	Reports show compliance with contextual information requirements and processes are in place to identify non-compliant, missing, or retired systems and applications.	Automated or technology-assisted processes and procedures exist to both create and remove systems and applications and associated attributes from the central repository, or data are correlated and reconciled with other systems that contain information about tracked systems and applications.
Identify	Automated	Infrastructure and applications are scanned ad-hoc or irregularly for vulnerability details, or vulnerability details are acquired from existing data repositories or from the systems themselves as time permits.	The process, configuration, and schedule for scanning infrastructure and applications is defined and followed for certain departments or divisions within the organization. Available technology may vary throughout the organization.	There are defined and mandated organization-wide scanning requirements and configurations for infrastructure and applications that set a minimum threshold for all departments or divisions. Technology is made available throughout the organization through enterprise licensing agreements or as a service.	Scanning coverage is measured and includes the measurement of authenticated vs. unauthenticated scanning (where applicable), the types of automated testing employed, false positive rates, and vulnerability escape rates.	Scanning is integrated into build-and-release processes and procedures and happens automatically in accordance with requirements. Scanning configurations and rules are updated based on previous measurements.
	Manual	Manual testing or review occurs when specifically required or requested.	Manual testing or review processes are established and some departments and divisions have defined requirements.	Manual testing or review occurs based on reasonable policy-defined requirements that apply to the entire organization and is available as a service where not specifically required by policy.	Deviations from manual testing or review requirements are tracked and reported.	Manual testing or review processes include focused testing based on historical test data and commonalities or threat intelligence.
	External	External vulnerability reports and disclosures are handled on a case-by-case basis.	Basic vulnerability disclosure policy (VDP) and contact information published, but backend processes and procedures not documented.	More comprehensive VDP in place, along with terms and conditions for external vendors and security researchers, that outlines rules of engagement, tracking, and feedback processes.	Compliance with VDP and terms and conditions is tracked and measured and information is used to streamline processes and evaluate vendors and researchers.	A mature external testing and research program is in place with specific goals and campaigns that may only be available to specific vendors or researchers.
Analyze	Prioritization	Prioritization is performed based on CVSS/Severity designations provided by identification technology or indicated in reports.	Prioritization also includes analysis of other available fields such as whether or not exploits or malware exist or confidence scores.	Prioritization includes correlation with the affected asset, asset group, or application to account for it's criticality in addition to the severity designation. This may require light to moderate customization depending on architecture and design.	Generic threat intelligence or other custom data, which may require additional products or services, are leveraged to perform prioritization.	Company-specific threat intelligence, or other information gathered from the operating environment, is leveraged to preform prioritization. This information may require human analysis or more extensive customization.
	Root Cause Analysis	Root cause analysis is performed based on out-of-the-box information such as standard remediation/patch reports or other categorized reports (e.g., OWASP Top 10 category).	Data are lightly customized to apply less granular or more meaningful groupings of data than CVE, CWE, or Top 10 identifiers to facilitate root cause analysis.	Data are also identified, grouped, and/or filtered by department or location to enable identification of location- or group-based deficiencies. This may require light to moderate customization depending on architecture and design.	Data are also identified, grouped, and/or filtered by owner or role. This may require more extensive customization and ongoing maintenance.	An executive dashboard is in place and includes the highest-risk root cause impediments, exclusions, project cost projections, etc. This will require more detailed analysis and customization to become meaningful and should integrate with existing executive business intelligence tools.
Communicate	Metrics & Reporting	Simple, point-in-time operational metrics are available primarily sourced from out-of-the-box reports leveraging minimal customization or filtering.	Filtered reports are created to target specific groups or prioritize findings. Specific divisions or departments have defined their own reporting requirements, including both program and operational metrics, and generate and release the corresponding reports at a defined interval.	Reporting requirements, including all required program, operational, and executive metrics and trends, are well-defined and baseline reports are consistent throughout the organization and tailored or filtered to the individual departments or stakeholders.	Reports and metrics include an indication of compliance with defined policy and standards, treatment timelines, and bug bars. Correlation with other security or contextual data sources allows for more meaningful grouping, improves accuracy, and allows for identification of faulty or inefficient design patterns.	Custom reporting is available as a service or via self-service options, or feedback is regularly solicited and reports are updated to reflect changing needs. Automated outlier and trend analysis along with exclusion tracking is performed to identify high/low performers and highlight systemic issues/successes.
	Alerting	Alerting is either not available or only available within security-specific technologies.	Integrations exist and alerts are being sent for specific divisions or departments or for users of specific non-security technologies already being leveraged by some stakeholders.	Alerting is available for most stakeholders in their technology of choice.	Visibility and both timing and detail of response to alerts is measured and tracked.	Data are analyzed to develop a standard or automated response to alerts for common issues that can be tied to a common response.
Treat	Change Management	Changes related to vulnerability management activities pass through the same workflow as any other change.	Some changes related to vulnerability management activities have a custom workflow or are treated as standard changes.	Most changes related to vulnerability management activities follow a custom workflow or are treated as standard changes.	Changes related to vulnerability management activities along with success rates are tracked. Timing is also measured for different stages of the change or subtasks related to the change.	Metrics from vulnerability management change activities are used to modify requirements or streamline future change requests. At least some standard changes are automated.
	Patch Management	Patches are applied manually or scheduled by admins and end-users.	There is a standard schedule defined and technology is available for some divisions or departments or for some platforms to automate patch testing and deployment.	All departments are required to patch within a certain timeframe and technologies are available to assist with testing and applying patches for all approved platforms.	Patch management activities are tracked along with compliance with remediation timelines and the success rate.	Data from patch management activities, security incidents, and threat intelligence are used to right-size remediation timelines and identify process or technology changes.
	Configuration Management	Configuration requirements are not well-defined and changes are either applied manually or the automatic application of configurations is only available for a subset of platforms.	Configurations are defined for some divisions or departments or for specific platforms.	Configurations are defined for all supported platforms and technologies are available to automate or validate configuration changes for all platforms.	Deviations from configuration requirements and associated service impacts are measured and tracked.	Data from the configuration process along with security incidents and threat intelligence are leveraged to strengthen or relax requirements as needed.

Source: SANS

Welke Resources naast SANS kan ik nog nog meer gebruiken

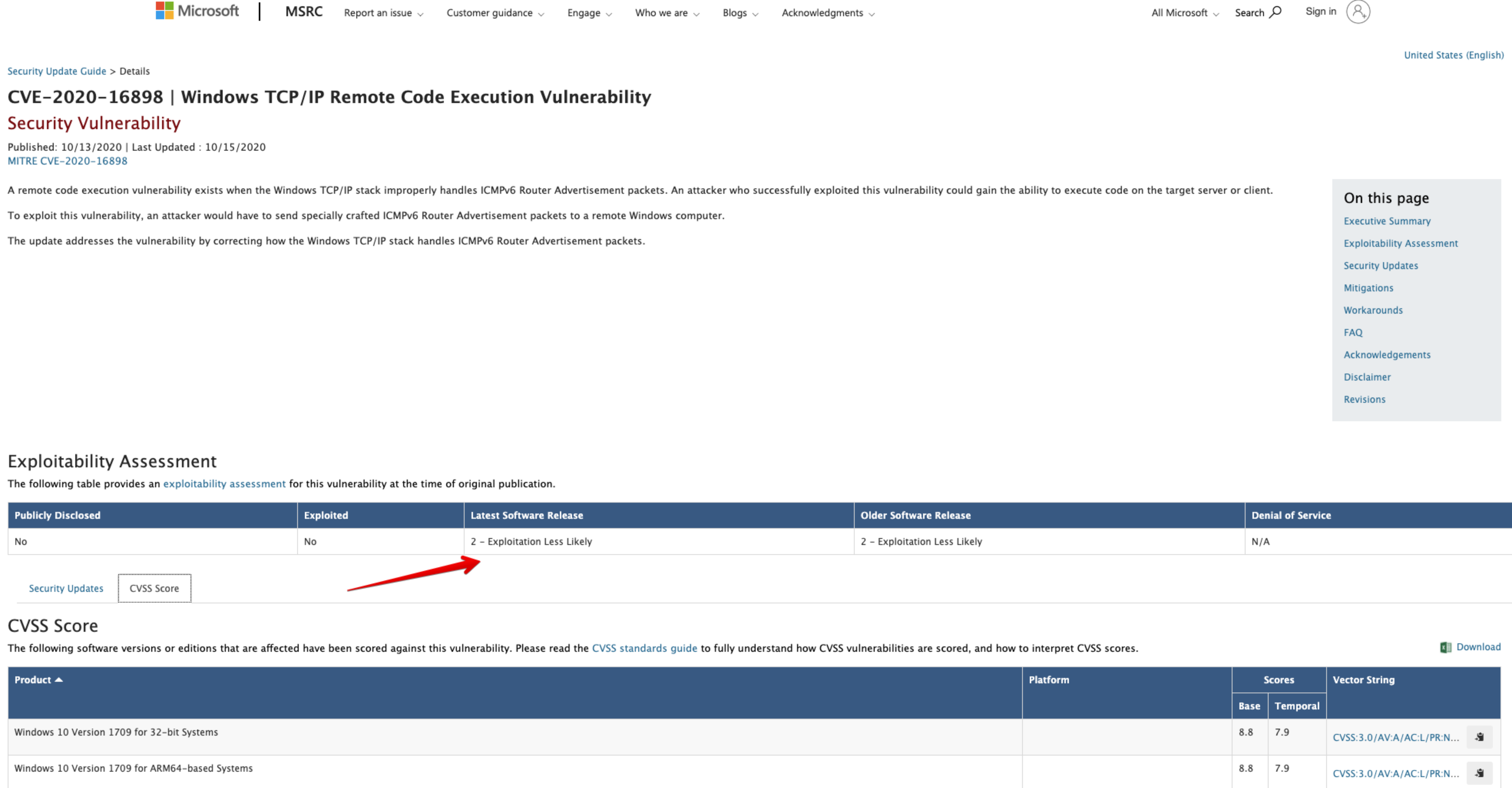


Vulnerability Responses

Large scale security vulnerabilities like the ones below receive special attention from Red Hat Product Security. In order to create the best experience possible for our customers during these critical moments, a specialized vulnerability page is created within the Red Hat Product Security Center which aggregates information, diagnostic tools, and updates in one easy-to-use interface. This list is a catalog of these pages.

A full list of all CVEs affecting Red Hat Products can be found in our CVE Database.

Alias / CVE	Impact	Status	Public Date ▾
BleedingTooth - Kernel Bluetooth vulnerabilities - CVE-2020-12351, CVE-2020-12352, and CVE-2020-24490	Important	Ongoing	14 Oct 2020
Boot Hole Vulnerability - GRUB 2 boot loader - CVE-2020-10713	Moderate	Ongoing	29 Jul 2020
Runc regression - docker-1.13.1-108 - CVE-2016-8867, CVE-2020-14298, and CVE-2020-14300	Important	✓ Resolved	23 Jun 2020
CVE-2020-11100 haproxy: malformed HTTP/2 requests can lead to out-of-bounds writes	Critical	✓ Resolved	02 Apr 2020
Machine Check Error on Page Size Change - CVE-2018-12207	Important	✓ Resolved	12 Nov 2019
VHOST-NET GUEST TO HOST ESCAPE - Kernel vulnerability - CVE-2019-14835	Important	✓ Resolved	17 Sep 2019
TCP SACK PANIC - Kernel vulnerabilities - CVE-2019-11477, CVE-2019-11478 & CVE-2019-11479	Important	✓ Resolved	17 Jun 2019
MDS - Microarchitectural Data Sampling - CVE-2018-12130, CVE-2018-12126, CVE-2018-12127, and CVE-2019-11091	Important	✓ Resolved	14 May 2019
runc - Malicious container escape - CVE-2019-5736	Important	✓ Resolved	11 Feb 2019
Kubernetes privilege escalation and access to sensitive information in OpenShift products and services - CVE-2018-1002105	Critical	✓ Resolved	03 Dec 2018
Mutagen Astronomy - Local privilege escalation - CVE-2018-14634	Important	✓ Resolved	25 Sep 2018
L1TF - L1 Terminal Fault Attack - CVE-2018-3620 & CVE-2018-3646	Important	✓ Resolved	14 Aug 2018



Security Update Guide > Details

CVE-2020-16898 | Windows TCP/IP Remote Code Execution Vulnerability

Security Vulnerability

Published: 10/13/2020 | Last Updated : 10/15/2020
MITRE CVE-2020-16898

A remote code execution vulnerability exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets. An attacker who successfully exploited this vulnerability could gain the ability to execute code on the target server or client.

To exploit this vulnerability, an attacker would have to send specially crafted ICMPv6 Router Advertisement packets to a remote Windows computer.

The update addresses the vulnerability by correcting how the Windows TCP/IP stack handles ICMPv6 Router Advertisement packets.

On this page

- Executive Summary
- Exploitability Assessment
- Security Updates
- Mitigations
- Workarounds
- FAQ
- Acknowledgements
- Disclaimer
- Revisions

Exploitability Assessment

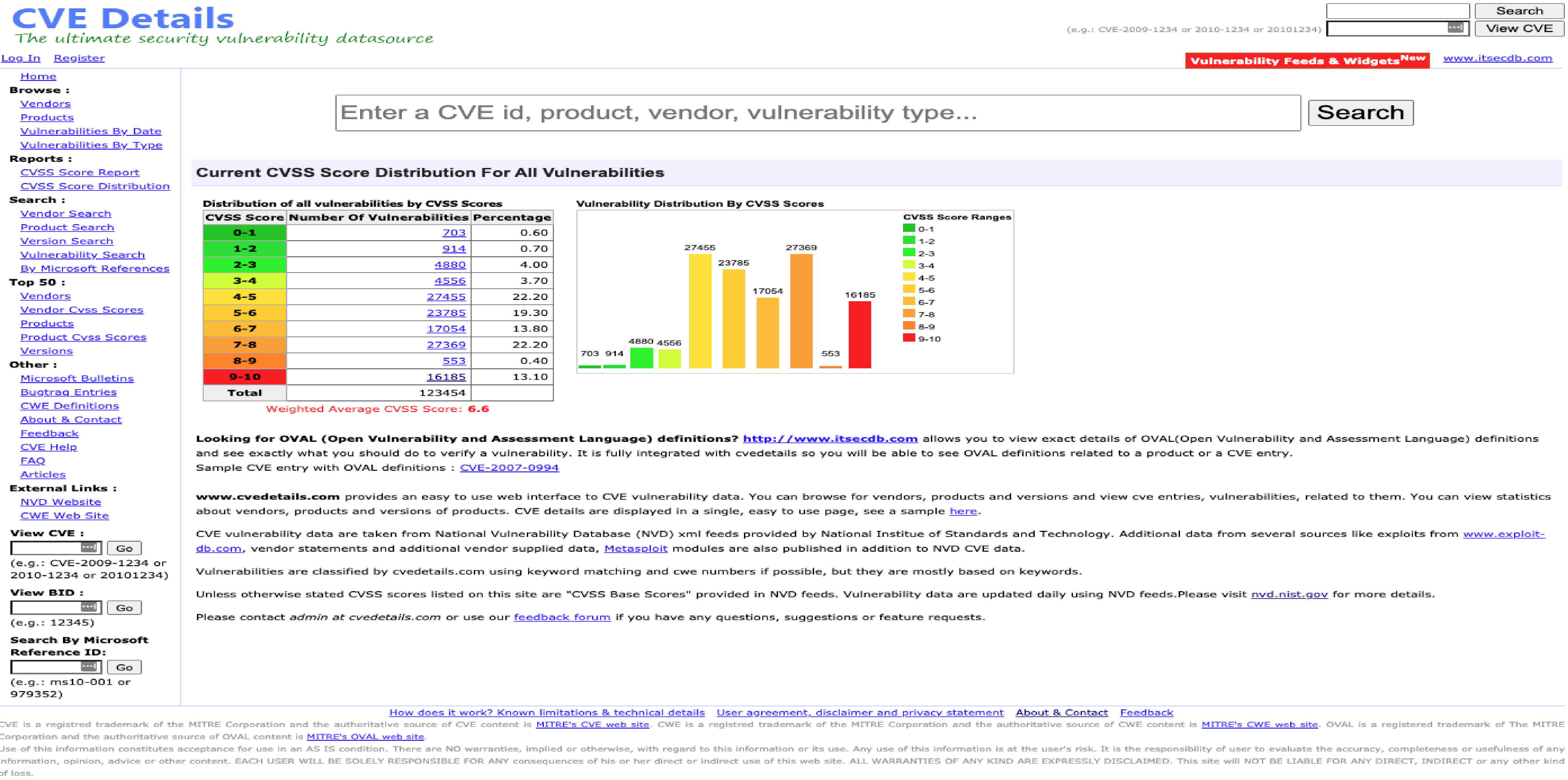
The following table provides an exploitability assessment for this vulnerability at the time of original publication.

Publicly Disclosed	Exploited	Latest Software Release	Older Software Release	Denial of Service
No	No	2 - Exploitation Less Likely	2 - Exploitation Less Likely	N/A

CVSS Score

The following software versions or editions that are affected have been scored against this vulnerability. Please read the CVSS standards guide to fully understand how CVSS vulnerabilities are scored, and how to interpret CVSS scores.

Product ▲	Platform	Scores		Vector String
		Base	Temporal	
Windows 10 Version 1709 for 32-bit Systems		8.8	7.9	CVSS:3.0/AV:A/AC:L/PR:N...
Windows 10 Version 1709 for ARM64-based Systems		8.8	7.9	CVSS:3.0/AV:A/AC:L/PR:N...



CVE Details

The ultimate security vulnerability datasource

Search
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)
View CVE
Log In
Register
Vulnerability Feeds & Widgets New
www.itsecdb.com

- 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 :**
  - Microsoft Bulletins
  - Bugtraq Entries
  - CWE Definitions
  - About & Contact
  - Feedback
  - CVE Help
  - FAQ
  - Articles
- **External Links :**
  - NVD Website
  - CWE Web Site

View CVE : Go
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View BID : Go
(e.g.: 12345)

Search By Microsoft Reference ID: Go
(e.g.: ms10-001 or 979352)

Current CVSS Score Distribution For All Vulnerabilities

Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	703	0.60
1-2	914	0.70
2-3	4880	4.00
3-4	4556	3.70
4-5	27455	22.20
5-6	23785	19.30
6-7	17054	13.80
7-8	27369	22.20
8-9	553	0.40
9-10	16185	13.10
Total	123454	

Weighted Average CVSS Score: **6.6**

Vulnerability Distribution By CVSS Scores

Looking for OVAL (Open Vulnerability and Assessment Language) definitions? http://www.itsecdb.com allows you to view exact details of OVAL(Open Vulnerability and Assessment Language) definitions and see exactly what you should do to verify a vulnerability. It is fully integrated with cvedetails so you will be able to see OVAL definitions related to a product or a CVE entry.
Sample CVE entry with OVAL definitions : CVE-2007-0994

www.cvedetails.com provides an easy to use web interface to CVE vulnerability data. You can browse for vendors, products and versions and view cve entries, vulnerabilities, related to them. You can view statistics about vendors, products and versions of products. CVE details are displayed in a single, easy to use page, see a sample here.

CVE vulnerability data are taken from National Vulnerability Database (NVD) xml feeds provided by National Institue of Standards and Technology. Additional data from several sources like exploits from www.exploit-db.com, vendor statements and additional vendor supplied data, Metasploit modules are also published in addition to NVD CVE data.

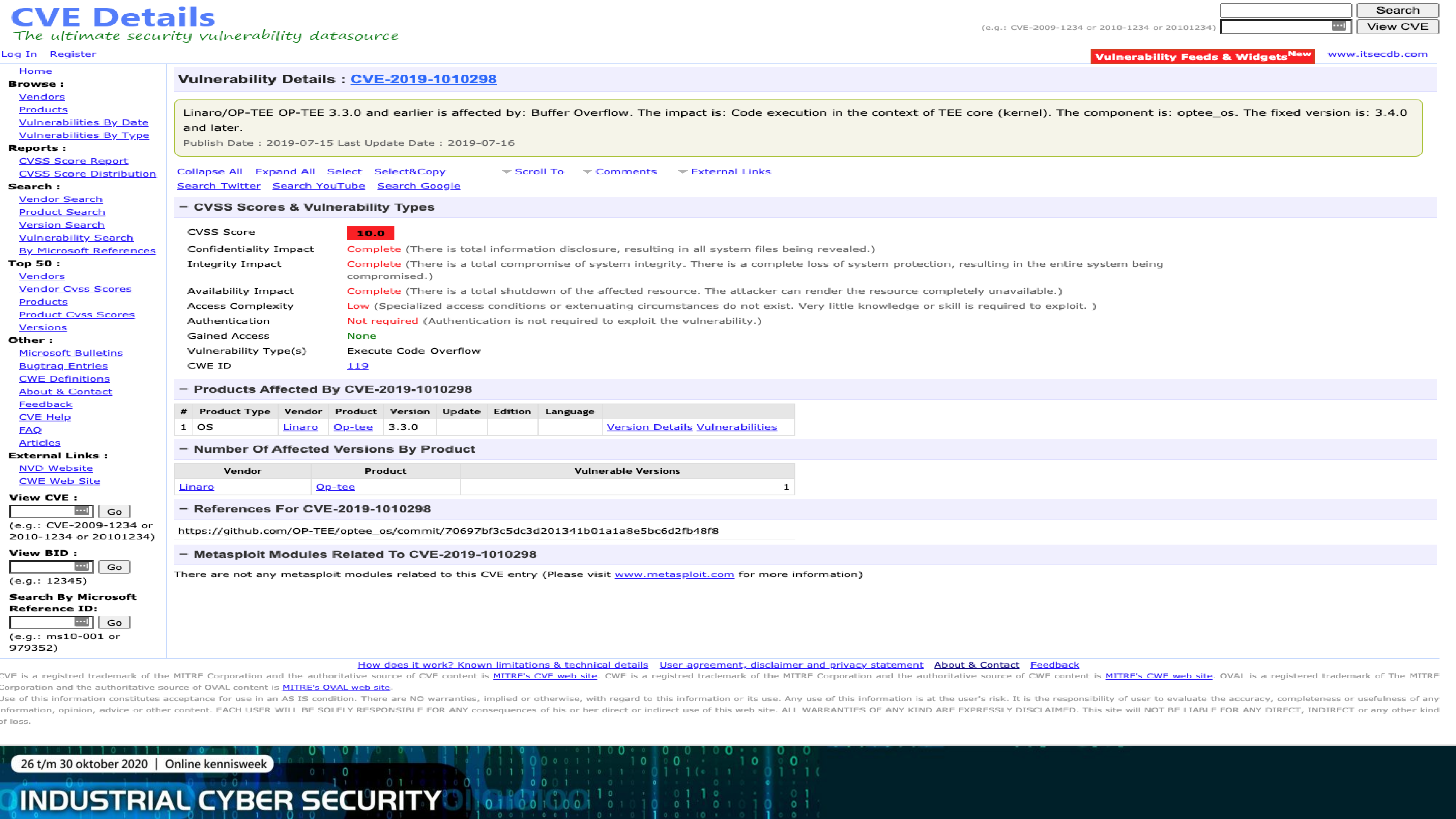
Vulnerabilities are classified by cvedetails.com using keyword matching and cwe numbers if possible, but they are mostly based on keywords.

Unless otherwise stated CVSS scores listed on this site are "CVSS Base Scores" provided in NVD feeds. Vulnerability data are updated daily using NVD feeds.Please visit nvd.nist.gov for more details.

Please contact *admin at cvedetails.com* or use our feedback forum if you have any questions, suggestions or feature requests.

How does it work? Known limitations & technical details User agreement, disclaimer and privacy statement About & Contact Feedback

CVE is a registred trademark of the MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. CWE is a registred trademark of the MITRE Corporation and the authoritative source of CWE content is MITRE's CWE web site. OVAL is a registered trademark of The MITRE Corporation and the authoritative source of OVAL content is MITRE's OVAL web site.
Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.



CVE Details

The ultimate security vulnerability datasource

Search
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)
View CVE
Log In
Register
Vulnerability Feeds & Widgets New
www.itsecdb.com

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 :
- Microsoft Bulletins
- Bugtraq Entries
- CWE Definitions
- About & Contact
- Feedback
- CVE Help
- FAQ
- Articles

External Links :
- NVD Website
- CWE Web Site

View CVE :

Go

(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)

View BID :

Go

(e.g.: 12345)

Search By Microsoft Reference ID:

Go

(e.g.: ms10-001 or 979352)

Vulnerability Details : CVE-2019-1010298

Linaro/OP-TEE OP-TEE 3.3.0 and earlier is affected by: Buffer Overflow. The impact is: Code execution in the context of TEE core (kernel). The component is: optee_os. The fixed version is: 3.4.0 and later.

Publish Date : 2019-07-15 Last Update Date : 2019-07-16

− CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code Overflow
CWE ID	119

− Products Affected By CVE-2019-1010298

#	Product Type	Vendor	Product	Version	Update	Edition	Language	
1	OS	Linaro	Op-tee	3.3.0				Version Details Vulnerabilities

− Number Of Affected Versions By Product

Vendor	Product	Vulnerable Versions
Linaro	Op-tee	1

− References For CVE-2019-1010298

https://github.com/OP-TEE/optee_os/commit/70697bf3c5dc3d201341b01a1a8e5bc6d2fb48f8

− Metasploit Modules Related To CVE-2019-1010298

There are not any metasploit modules related to this CVE entry (Please visit www.metasploit.com for more information)

Uit welke componenten bestaat een “VM” architectuur uit in een IT / OT Landscap

Architectuur in Security Landschap

Firewall Integration

SIEM Integration

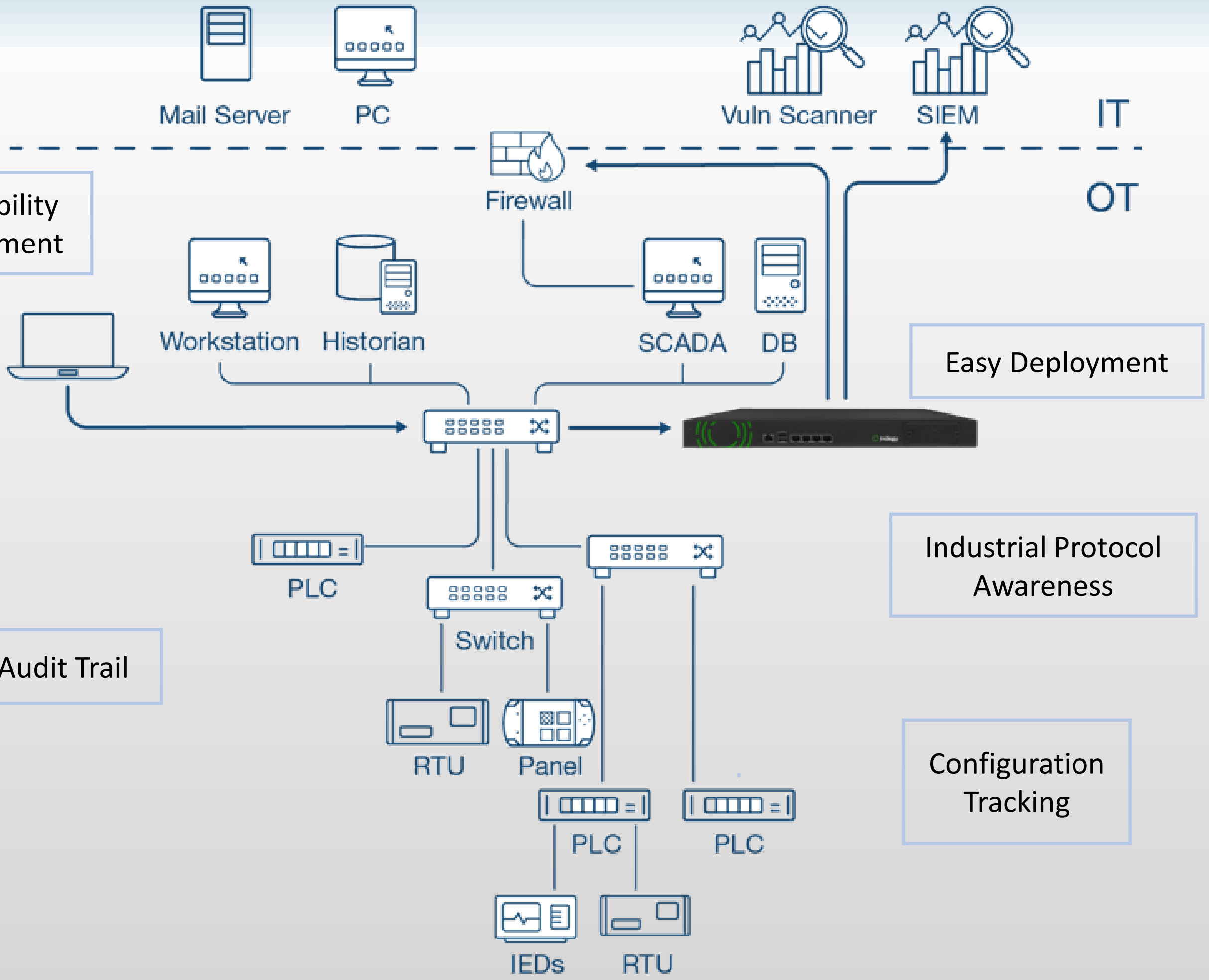
Vulnerability Management

Easy Deployment

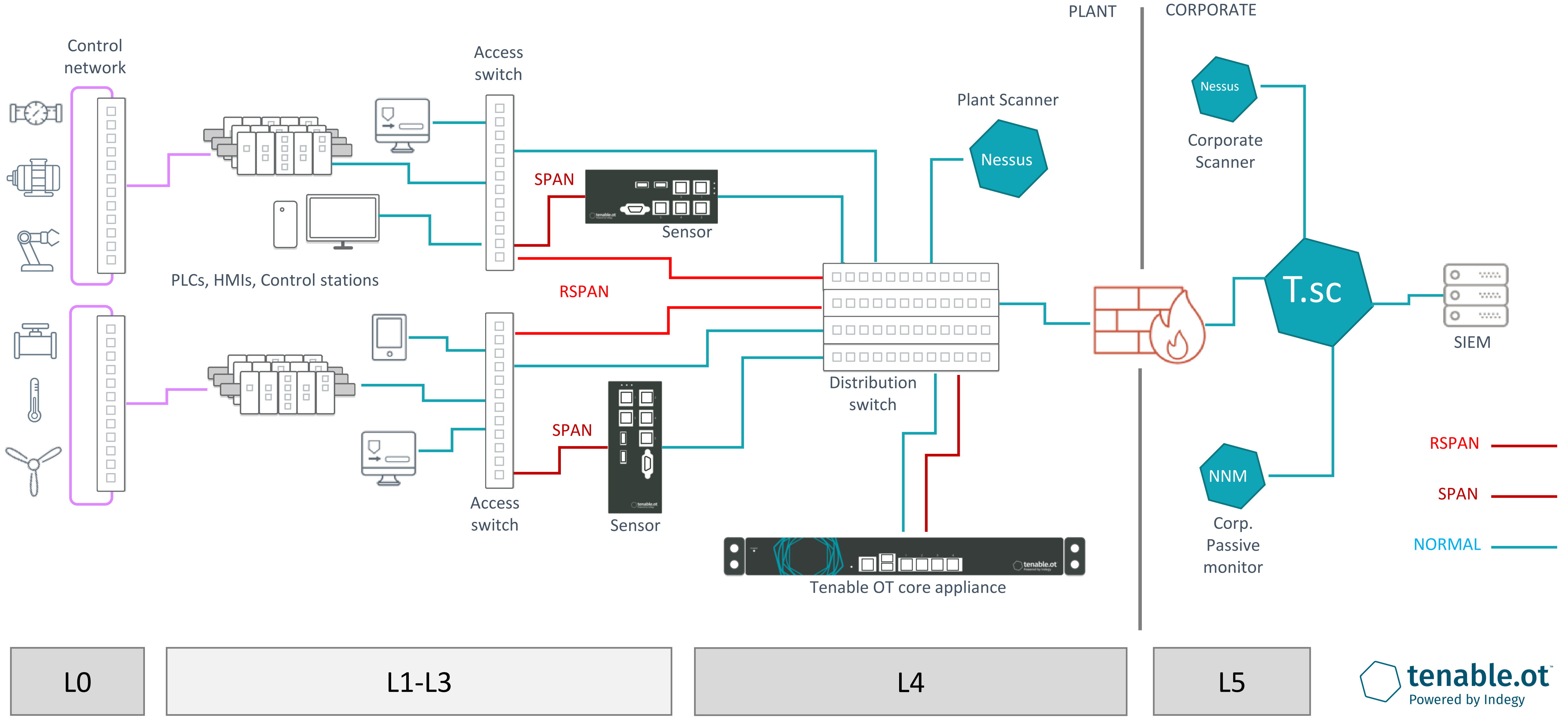
Industrial Protocol Awareness

OT Audit Trail

Configuration Tracking



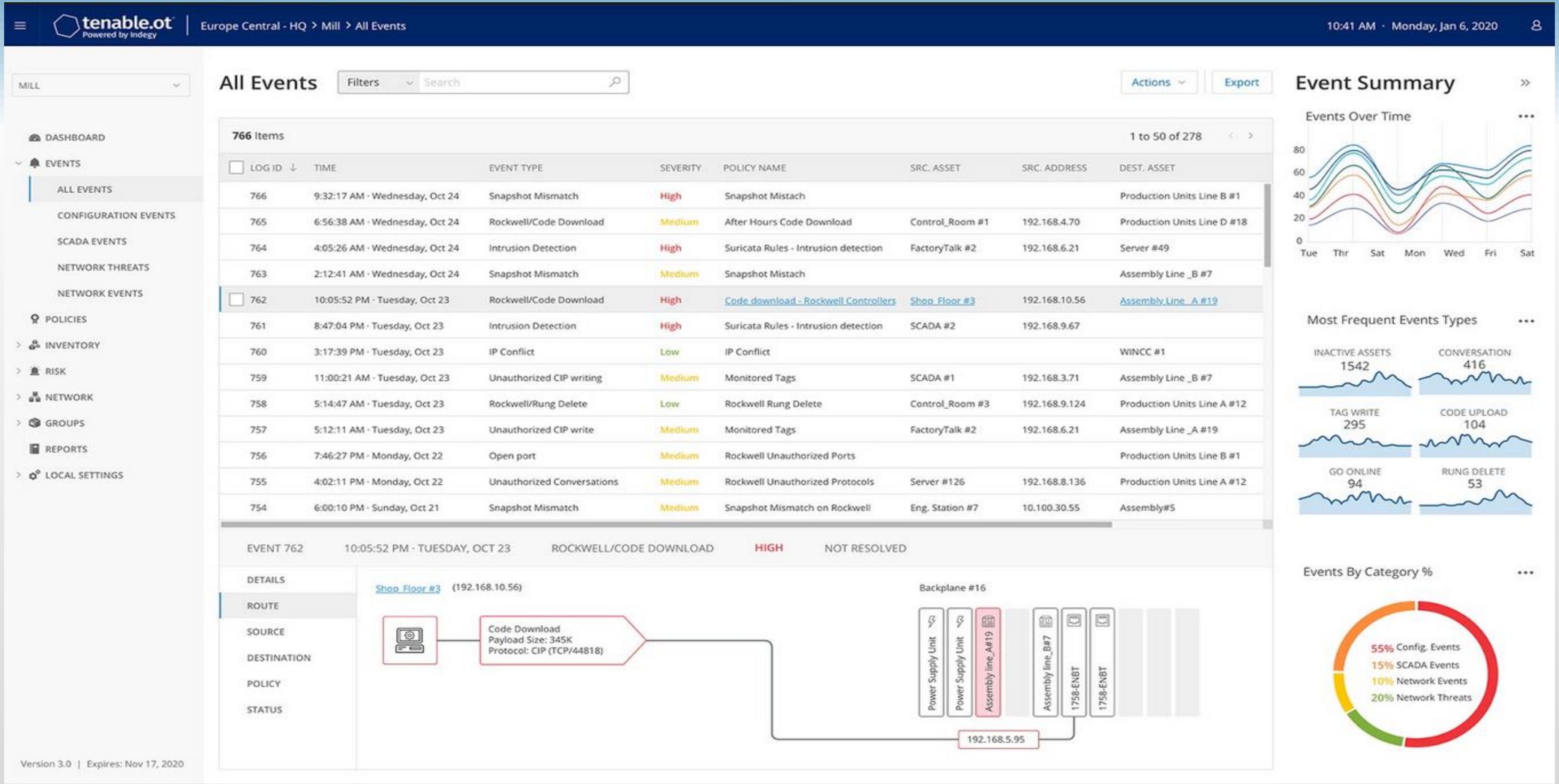
Tenable.ot Solutions Architecture



tenable.ot
Powered by Indegy

Voorbeeld Dashboards

IT vs OT risks



All Events

766 Items — 1 to 50 of 278

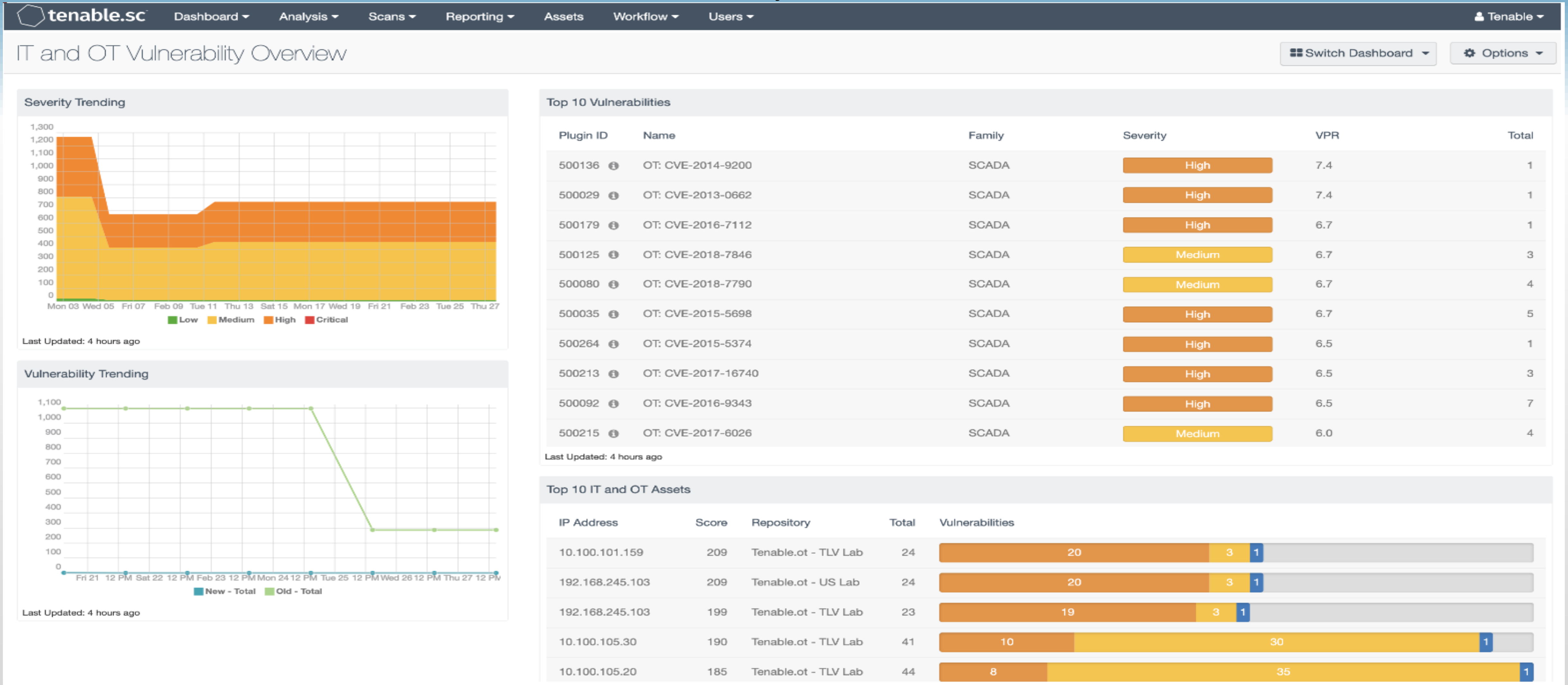
LOG ID	TIME	EVENT TYPE	SEVERITY	POLICY NAME	SRC. ASSET	SRC. ADDRESS	DEST. ASSET
766	9:32:17 AM · Wednesday, Oct 24	Snapshot Mismatch	High	Snapshot Mistach			Production Units Line B #1
765	6:56:38 AM · Wednesday, Oct 24	Rockwell/Code Download	Medium	After Hours Code Download	Control_Room #1	192.168.4.70	Production Units Line D #18
764	4:05:26 AM · Wednesday, Oct 24	Intrusion Detection	High	Suricata Rules - Intrusion detection	FactoryTalk #2	192.168.6.21	Server #49
763	2:12:41 AM · Wednesday, Oct 24	Snapshot Mismatch	Medium	Snapshot Mistach			Assembly Line _B #7
762	10:05:52 PM · Tuesday, Oct 23	Rockwell/Code Download	High	Code download - Rockwell Controllers	Shop_Floor #3	192.168.10.56	Assembly Line _A #19
761	8:47:04 PM · Tuesday, Oct 23	Intrusion Detection	High	Suricata Rules - Intrusion detection	SCADA #2	192.168.9.67	
760	3:17:39 PM · Tuesday, Oct 23	IP Conflict	Low	IP Conflict			WINCC #1
759	11:00:21 AM · Tuesday, Oct 23	Unauthorized CIP writing	Medium	Monitored Tags	SCADA #1	192.168.3.71	Assembly Line _B #7
758	5:14:47 AM · Tuesday, Oct 23	Rockwell/Rung Delete	Low	Rockwell Rung Delete	Control_Room #3	192.168.9.124	Production Units Line A #12
757	5:12:11 AM · Tuesday, Oct 23	Unauthorized CIP write	Medium	Monitored Tags	FactoryTalk #2	192.168.6.21	Assembly Line _A #19
756	7:46:27 PM · Monday, Oct 22	Open port	Medium	Rockwell Unauthorized Ports			Production Units Line B #1
755	4:02:11 PM · Monday, Oct 22	Unauthorized Conversations	Medium	Rockwell Unauthorized Protocols	Server #126	192.168.8.136	Production Units Line A #12
754	6:00:10 PM · Sunday, Oct 21	Snapshot Mismatch	Medium	Snapshot Mismatch on Rockwell	Eng. Station #7	10.100.30.55	Assembly#5

EVENT 762 10:05:52 PM · TUESDAY, OCT 23 ROCKWELL/CODE DOWNLOAD HIGH NOT RESOLVED

Shop_Floor #3 (192.168.10.56)

Code Download
Payload Size: 345K
Protocol: CIP (TCP/44818)

Unified Vulnerability & Risico Overzicht


tenable.sc
Dashboard ▾
Analysis ▾
Scans ▾
Reporting ▾
Assets
Workflow ▾
Users ▾
Tenable ▾
IT and OT Vulnerability Overview
Switch Dashboard ▾
Options ▾
Severity Trending
1,300
1,200
1,100
1,000
900
800
700
600
500
400
300
200
100
0
Mon 03 Wed 05 Fri 07 Feb 09 Tue 11 Thu 13 Sat 15 Mon 17 Wed 19 Fri 21 Feb 23 Tue 25 Thu 27
🟩 Low 🟨 Medium 🟧 High 🟥 Critical
Last Updated: 4 hours ago
Vulnerability Trending
1,100
1,000
900
800
700
600
500
400
300
200
100
0
Fri 21 12 PM Sat 22 12 PM Feb 23 12 PM Mon 24 12 PM Tue 25 12 PM Wed 26 12 PM Thu 27 12 PM
🟦 New - Total 🟩 Old - Total
Last Updated: 4 hours ago

Top 10 Vulnerabilities

Plugin ID	Name	Family	Severity	VPR	Total
500136	OT: CVE-2014-9200	SCADA	High	7.4	1
500029	OT: CVE-2013-0662	SCADA	High	7.4	1
500179	OT: CVE-2016-7112	SCADA	High	6.7	1
500125	OT: CVE-2018-7846	SCADA	Medium	6.7	3
500080	OT: CVE-2018-7790	SCADA	Medium	6.7	4
500035	OT: CVE-2015-5698	SCADA	High	6.7	5
500264	OT: CVE-2015-5374	SCADA	High	6.5	1
500213	OT: CVE-2017-16740	SCADA	High	6.5	3
500092	OT: CVE-2016-9343	SCADA	High	6.5	7
500215	OT: CVE-2017-6026	SCADA	Medium	6.0	4

Last Updated: 4 hours ago

Top 10 IT and OT Assets

IP Address	Score	Repository	Total	Vulnerabilities
10.100.101.159	209	Tenable.ot - TLV Lab	24	20 3 1
192.168.245.103	209	Tenable.ot - US Lab	24	20 3 1
192.168.245.103	199	Tenable.ot - TLV Lab	23	19 3 1
10.100.105.30	190	Tenable.ot - TLV Lab	41	10 30 1
10.100.105.20	185	Tenable.ot - TLV Lab	44	8 35 1

Thank You

Jerry Zwanenburg, Sr. Security Engineer
gzwanenburg@tenable.com

Date: 28.10.2020

tenable