QSC24

Enhancing Cyber Resilience with Patchless Patching

Agenda

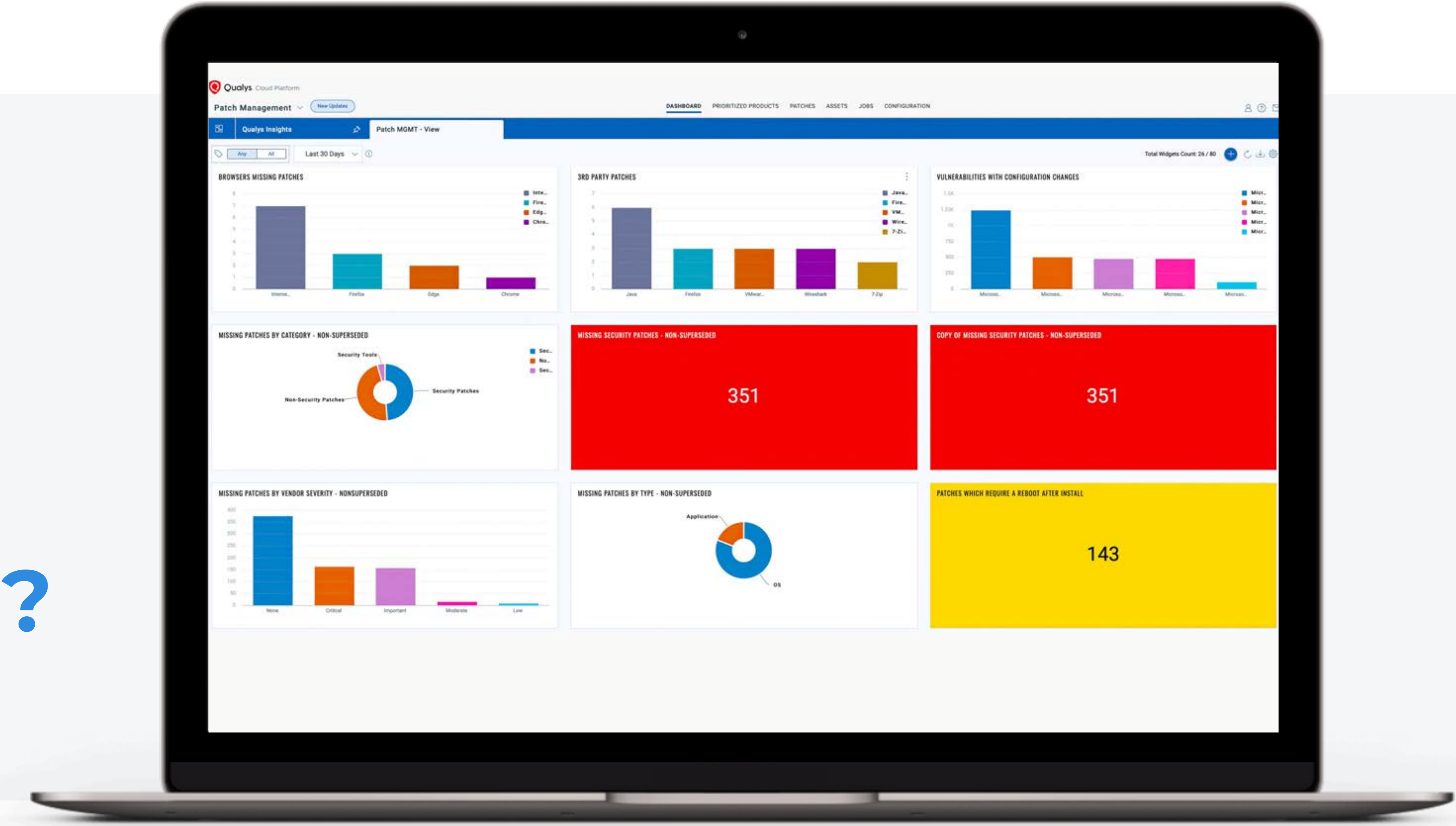
01 **The Goal:** Address more vulns, Faster

02 **Addressing vulns by patching:** While respecting Security – IT boundaries

03 **Success Story:** GE Vernova

04 **Addressing vulns without a patch:** Not all vulns can be patched

How Can We Be More **Efficient?**



National Cyber Security Centre

“A vulnerability management process shouldn’t exist in isolation. It is a cross-cutting effort and involves not just those working in IT operations, but also security and risk teams.”

The Fear of Downtime

Qualys.

More Open Vulnerabilities

More Patches to Deploy

Higher Chance of an Outage

Prioritize:

Focus on the vulnerabilities that count

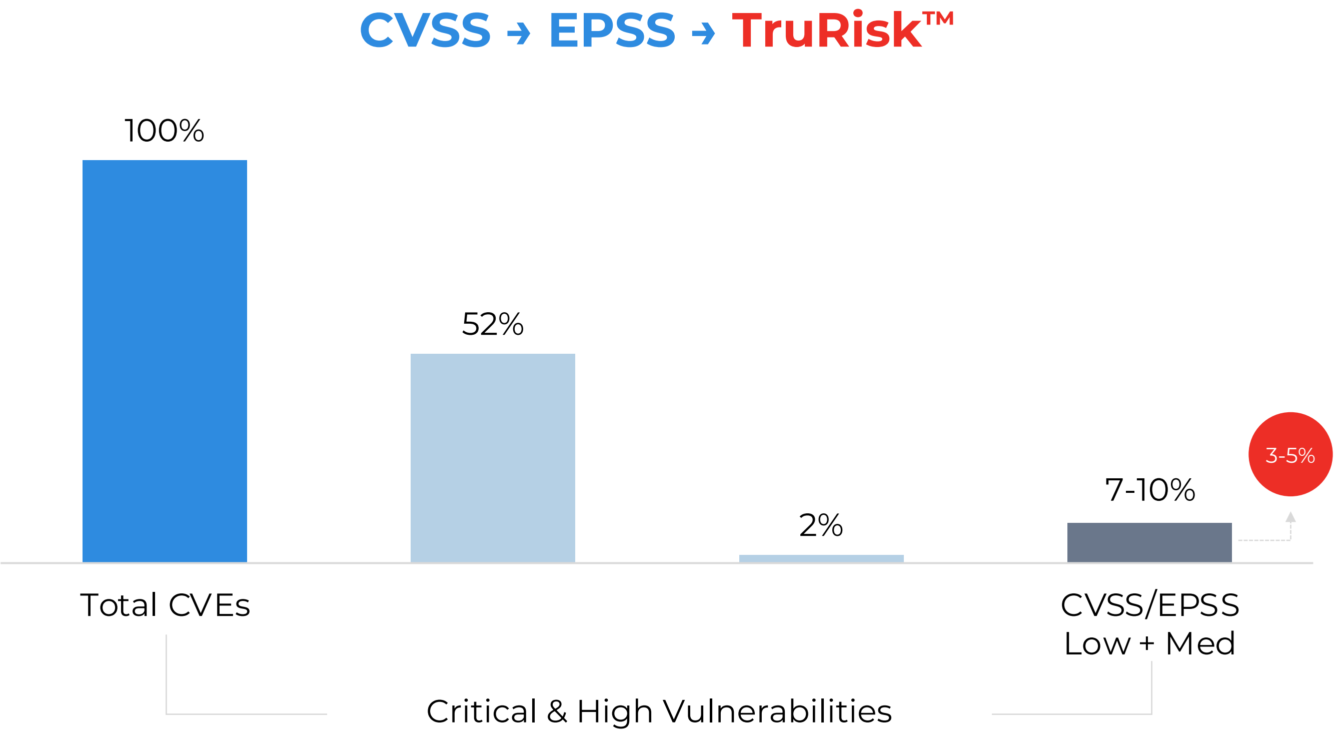
Use the Right Prioritization Method

Cut 52% to **<10% with TruRisk™**

CVSS
Too Many

EPSS
Too Few

TruRisk™
Just Right!



Patch Management

Qualys®

78M

Patches Deployed
Since Jan 2024

24 Days

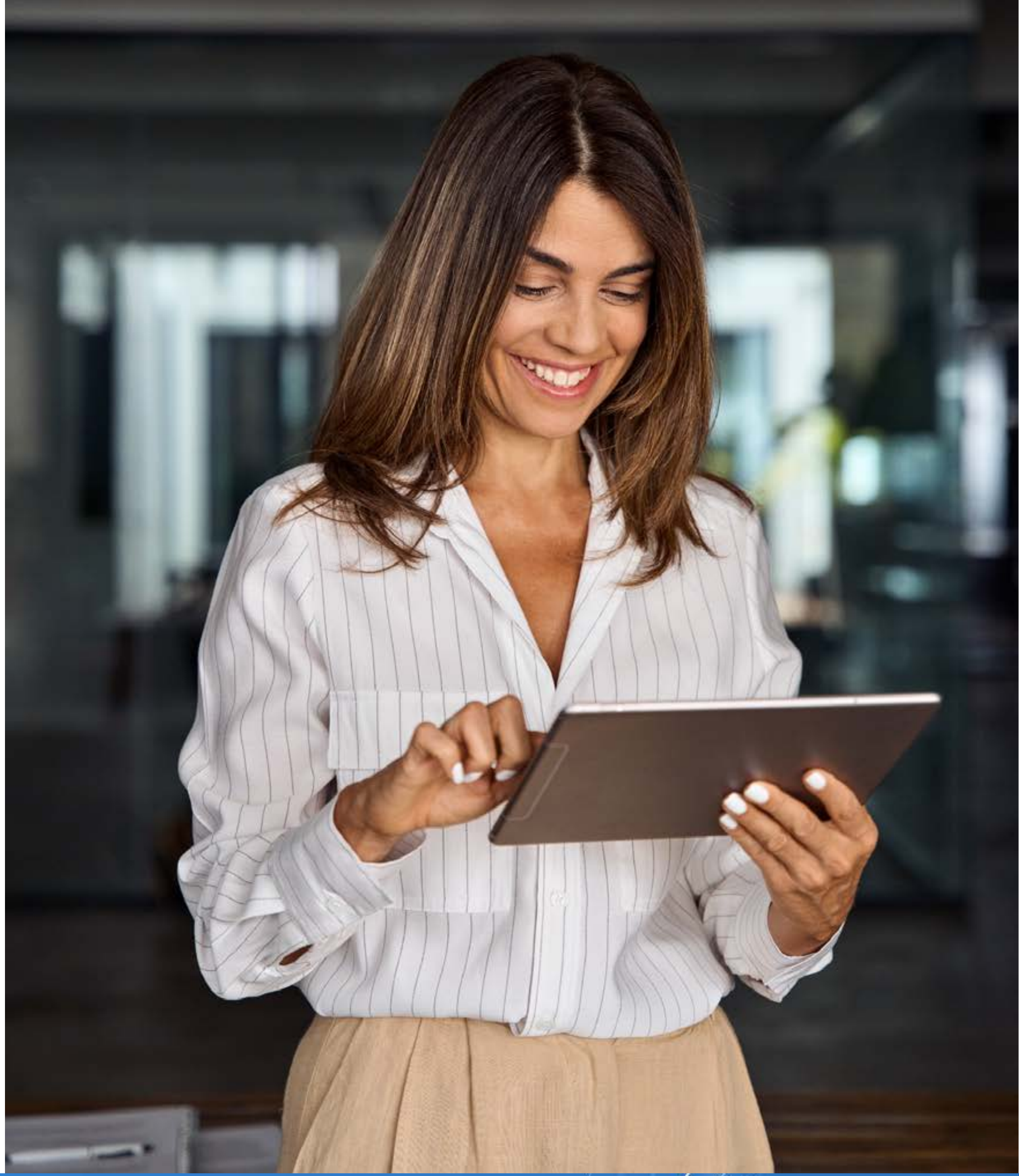
Faster remediation
of CISA KEV Vulns

160M

CISA KEV Vulns
Remediation with
Qualys Patch

Smart Automation

for your Prioritized Low Hanging Fruit Vulnerabilities



Smart Automation

Automate Low Hanging Fruit

Make sure products that introduce low risk of breaking when patched are always up to date

Focus on High-Risk High Reward Products

Identify products that introduce the most risk to your environment and focus on those first

Automate Based on Risk Where Possible

Automatically patch assets if a ransomware related vuln is detected, a CISA related one etc.

Minimize IT – SecOps Communication Friction

Automate the What & How

Let the Product Do the Research for You

Find the right patches and configuration changes required to remediate vulnerabilities

Ready to Be Deployed

Patches and configuration changes are packaged and ready to be deployed

Don’t Waste Remediation’s Team’s Time

Provide IT with an accurate list of patches and configuration changes required to remediate prioritized vulns

Separation of Duty

Follow patching best practices

Test & Deploy

Separation of Duty

Security teams prioritizes vulns, remediation teams test, approve and deploy patches and configuration changes

Test, Approve, Deploy & Rollback

Fully integrated with current IT best practices & tools

Automated Deployment with Testing

Automate “rings” to deploy patches & conf changes where possible

GE VERNOVA

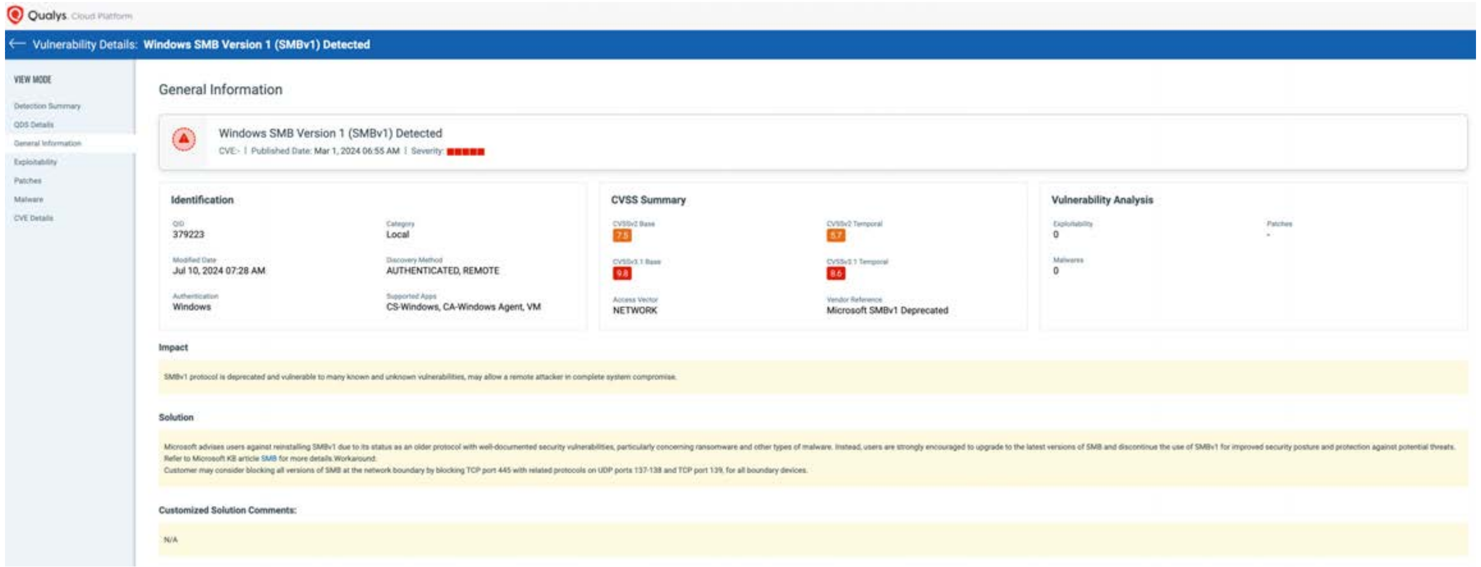
Corey Amsler

Director

Risk Management - EVM

Not all vulnerabilities can be patched!

Some Vulnerabilities Cannot Be Remediated with a Patch Because There Is No Patch



← Vulnerability Details: **Windows SMB Version 1 (SMBv1) Detected**

General Information

Windows SMB Version 1 (SMBv1) Detected
CVE: - | Published Date: Mar 1, 2024 06:55 AM | Severity: 🟥🟥🟥🟥🟥

Identification

QID
379223

Category
Local

Modified Date
Jul 10, 2024 07:28 AM

Discovery Method
AUTHENTICATED, REMOTE

Authentication
Windows

Supported Apps
CS-Windows, CA-Windows Agent, VM

CVSS Summary

CVSSv2 Base
7.5

CVSSv2 Temporal
5.7

CVSSv3.1 Base
9.8

CVSSv3.1 Temporal
8.6

Access Vector
NETWORK

Vendor Reference
Microsoft SMBv1 Deprecated

Vulnerability Analysis

Exploitability
0

Patches
-

Malwares
0

Impact

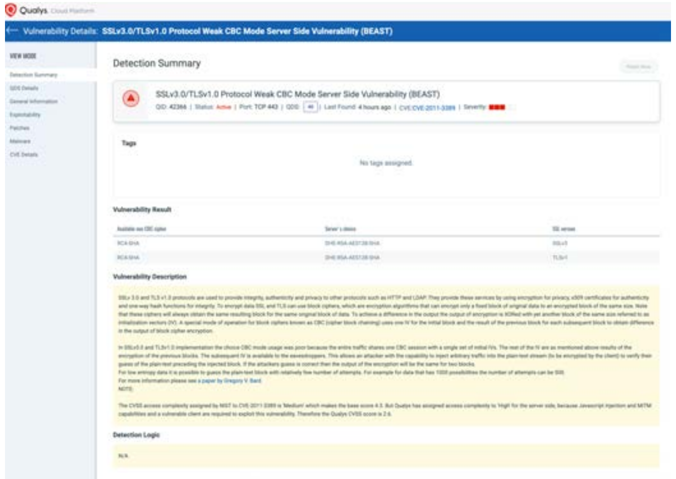
SMBv1 protocol is deprecated and vulnerable to many known and unknown vulnerabilities, may allow a remote attacker in complete system compromise.

Solution

Microsoft advises users against reinstalling SMBv1 due to its status as an older protocol with well-documented security vulnerabilities, particularly concerning ransomware and other types of malware. Instead, users are strongly encouraged to upgrade to the latest versions of SMB and discontinue the use of SMBv1 for improved security posture and protection against potential threats.
Refer to Microsoft KB article SMB for more details.Workaround:
Customer may consider blocking all versions of SMB at the network boundary by blocking TCP port 445 with related protocols on UDP ports 137-138 and TCP port 139, for all boundary devices.

Customized Solution Comments:

N/A



← Vulnerability Details: **SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST)**

Detection Summary

SSLv3.0/TLSv1.0 Protocol Weak CBC Mode Server Side Vulnerability (BEAST)
QID: 42366 | Status: Active | Port: TCP 443 | QDS: 40 | Last Found: 4 hours ago | CVE: CVE-2011-3389 | Severity: 🟥🟥🟥

Tags

No tags assigned.

Vulnerability Result

Available ssl CBC cipher	Server's choice	SSL version
RC4-SHA	DHE-RSA-AES128-SHA	SSLv3
RC4-SHA	DHE-RSA-AES128-SHA	TLSv1

Vulnerability Description

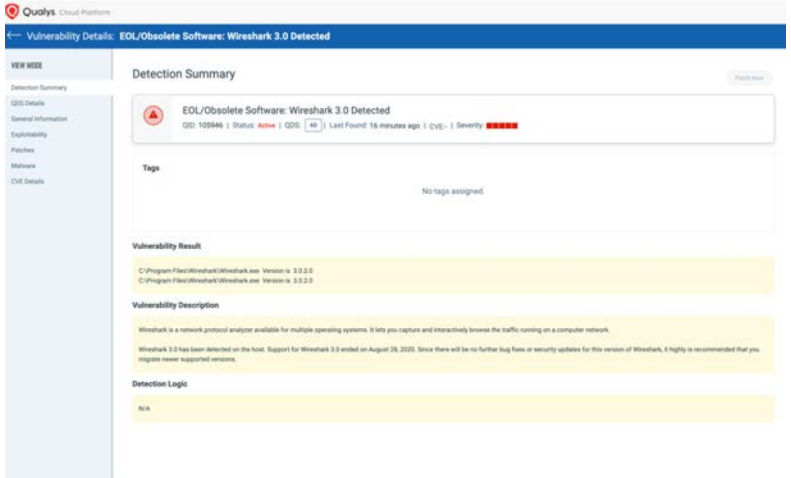
SSLv 3.0 and TLS v1.0 protocols are used to provide integrity, authenticity and privacy to other protocols such as HTTP and LDAP. They provide these services by using encryption for privacy, x509 certificates for authenticity and one-way hash functions for integrity. To encrypt data SSL and TLS can use block ciphers, which are encryption algorithms that can encrypt only a fixed block of original data to an encrypted block of the same size. Note that these ciphers will always obtain the same resulting block for the same original block of data. To achieve a difference in the output the output of encryption is XORed with yet another block of the same size referred to as initialization vectors (IV). A special mode of operation for block ciphers known as CBC (cipher block chaining) uses one IV for the initial block and the result of the previous block for each subsequent block to obtain difference in the output of block cipher encryption.

In SSLv3.0 and TLSv1.0 implementation the choice CBC mode usage was poor because the entire traffic shares one CBC session with a single set of initial IVs. The rest of the IV are as mentioned above results of the encryption of the previous blocks. The subsequent IV is available to the eavesdroppers. This allows an attacker with the capability to inject arbitrary traffic into the plain-text stream (to be encrypted by the client) to verify their guess of the plain-text preceding the injected block. If the attackers guess is correct then the output of the encryption will be the same for two blocks.
For low entropy data it is possible to guess the plain-text block with relatively few number of attempts. For example for data that has 1000 possibilities the number of attempts can be 500.
For more information please see a paper by Gregory V. Bard.
NOTE:

The CVSS access complexity assigned by NIST to CVE-2011-3389 is 'Medium' which makes the base score 4.3. But Qualys has assigned access complexity to 'High' for the server side, because Javascript injection and MITM capabilities and a vulnerable client are required to exploit this vulnerability. Therefore the Qualys CVSS score is 2.6.

Detection Logic

N/A



← Vulnerability Details: **EOL/Obsolete Software: Wireshark 3.0 Detected**

Detection Summary

EOL/Obsolete Software: Wireshark 3.0 Detected
QID: 105946 | Status: Active | QDS: 60 | Last Found: 16 minutes ago | CVE: - | Severity: 🟥🟥🟥🟥🟥

Tags

No tags assigned.

Vulnerability Result

C:\Program Files\Wireshark\Wireshark.exe Version is 3.0.2.0
C:\Program Files\Wireshark\Wireshark.exe Version is 3.0.2.0

Vulnerability Description

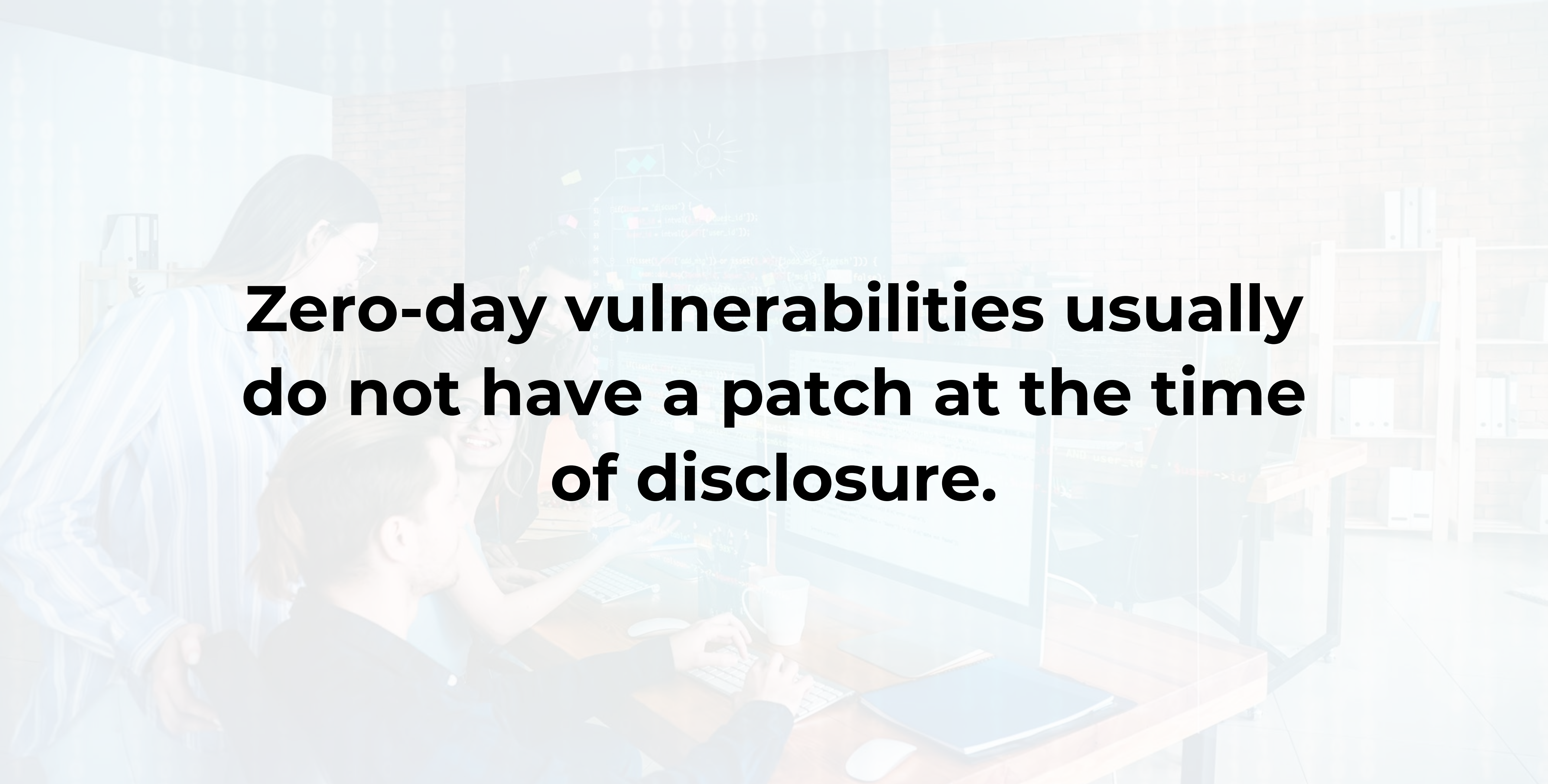
Wireshark is a network protocol analyzer available for multiple operating systems. It lets you capture and interactively browse the traffic running on a computer network.

Wireshark 3.0 has been detected on the host. Support for Wireshark 3.0 ended on August 28, 2020. Since there will be no further bug fixes or security updates for this version of Wireshark, it highly is recommended that you migrate newer supported versions.

Detection Logic

N/A

In some cases, patches cannot be deployed to production servers where service interruptions due to patching are not acceptable!



Zero-day vulnerabilities usually do not have a patch at the time of disclosure.

TruRisk Eliminate

Expanding Remediation Beyond Patching

Qualys®

TruRisk Eliminate

Patch + TruRisk Mitigate + TruRisk Isolate

Eliminate it, don’t just measure it.

TruRisk Mitigate

Fix Vulns That DO NOT Have a Patch

Map QIDs to Remediation Actions

Qualys prepares and tests the relevant configuration change or uninstall command to fix EOL vulnerable software

Customer can test and deploy the remediation actions to the vulnerable assets only using the Qualys agent

Vulnerabilities will be marked as closed in VMDR reports

Address Vulnerabilities That Cannot Be Patched Due to High Risk for an Outage

Map QIDs to Alternative Mitigations

- Qualys Threat Research prepares and validates mitigation options for critical vulns
- Mitigation techniques exemples: block ports, stop services, conf changes, Etc.
- Most mitigations can be easily rollbacked compared to rolling-back a patch
- Customer can test and deploy those mitigations instead of deploying the patch
- Mitigated status and risk reduction are reflected in all VMDR reports

Address Zero-day Vulns Until a Patch Is Available

Mitigation to Address a Zero-day

Qualys Threat Research prepares and validates a mitigation option

Customer can test and deploy the mitigation ASAP

Mitigated status and risk reduction are reflected in all VMDR reports

TruRisk Isolate

Device Isolation

As a Last Resort

- Isolate the device from the network
- Allow remote patching and control from Qualys and other allowed resources
- Agent technology – no EDR technology required

Fully Integrated with VMDR

Fully Integrated

Familiar Workflows

- Workflows for VMDR, patching, conf changes and mitigation are fully integrated providing same user experience

- All results are reflected in VMDR reports

Follow Up Session

Patch and Patchless Patching: Achieving Immediate Risk Reduction

Tomorrow 3:40PM

TruRisk Mitigate

Available: End of October 2024

TruRisk Isolate

Available: Q1 / 2025

Demo

Qualys®

Conclusion

Qualys®

Eliminate It, Don’t Just Measure It.

TruRisk **Eliminate**

Address All Types of Vulnerabilities

TruRisk Patch

- Test and deploy patches to fix vulns
- Fully automate patch deployment based on risk
- Windows, Mac, Linux OS and 3rd party app support

+

TruRisk Mitigate

- Remediate vulns that don’t have a patch
- Mitigate vulns that cannot be patched due to operational risk
- Address Zero Day vulns before the patch is available

+

TruRisk Isolate

- Isolate device to ensure vulns cannot be exploited
- Allow exceptions to ensure device can be patched and managed

TruRisk Eliminate

Map vulnerabilities to remediation and mitigation actions

Minimize MTTR

For all your critical vulnerabilities.

Better Collaboration

Between security and remediation teams – address vulnerabilities the way that best suits your teams

Fully Integrated

with VMDR and Patch workflows, reporting and UX

Focus on Risk Reduction

Prioritize and address all sorts of vulnerabilities based on their security risk

Qualys®

Q&A