tenable®

SOLUTION OVERVIEW

TENABLE APPLICATION SUITE FOR SERVICENOW

MANAGE YOUR CYBER EXPOSURE WITHIN SERVICENOW

Business Challenge

The attack surface and threat landscape are continuously changing, and organizations are constantly struggling with knowing their full picture of cyber risk when it comes to their IT, cloud and OT assets. The communication between security and IT teams is often limited due to the lack of having a centralized system to identify the most critical vulnerabilities and manage the remediation workflow process to stay on top of complex threats and growing security requirements. Without this tight integration, organizations are at risk with slow response times and poor visibility into their Cyber Exposure.

Solution

The Tenable™ integration with ServiceNow® offers best-in-class security by combining ServiceNow's industry-leading security orchestration, automation, and response engine with Tenable's market leading Cyber Exposure platform to quickly and effectively automate remediation response based on actual risk. The integrated solution provides a cohesive platform for both IT and security teams to streamline the vulnerability management, prioritization and remediation of all your organization's critical assets.

Value

The Tenable suite of ServiceNow apps provide:

Tenable Connector:

- A simple standardized library to configure how to connect to your Tenable platform(s)

Tenable for Assets:

- Bi-directional Asset Syncing between Tenable Platforms and ServiceNow CMDB

Tenable for IT Service Management:

- Bring Tenable Critical and High Severity findings into ServiceNow as incidents to start building out workflow/process

Tenable.ot for Vulnerability Response:

- Bring all of your Tenable OT Security findings into ServiceNow Vulnerability Response and leverage all the powerful pre-built functionality of Vulnerability Response

Vulnerability Response Integration with Tenable:

- Complementary application to Tenable.ot for Vulnerability Response to bring Tenable.io/Tenable.sc findings.

servicenow™

Technology Components

- Tenable.io/ Tenable.sc
- Tenable Connector
- Tenable for Assets
- Tenable for ITSM
- Tenable.ot for Vulnerability Response
- Vulnerability Response Integration with Tenable
- ServiceNow Rome, San Diego, Tokyo, Utah

Key Benefits

- Respond quickly, reduce errors through automation and orchestration
- Closed-loop remediation via targeted re-scans
- Reduce risk, exposure and loss by prioritizing the most critical vulnerabilities to fix first
- Improve operational efficiency with coordinated response across IT and security teams

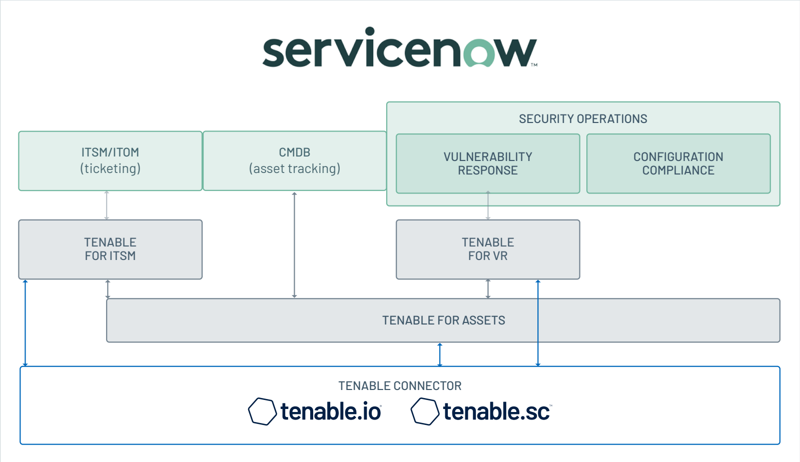
About Tenable

Tenable® is the Exposure Management company. More than 40,000 organizations around the globe rely on Tenable to understand and reduce cyber risk. As the creator of Nessus®, Tenable extended its expertise in vulnerabilities to deliver the world's first platform to see and secure any digital asset on any computing platform. Tenable customers include approximately 60 percent of the Fortune 500, approximately 40 percent of the Global 2000, and large government agencies. Learn more at www.tenable.com.

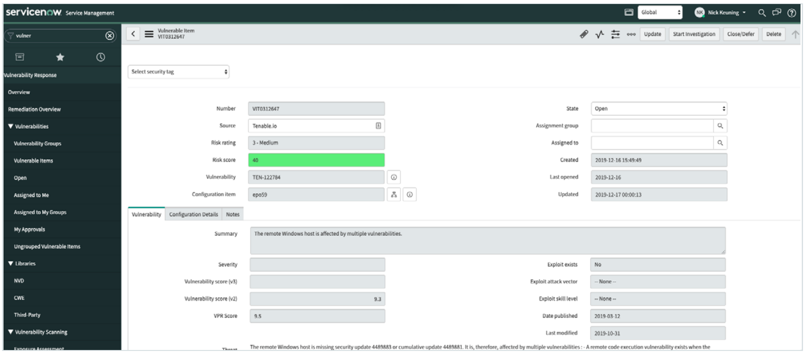
About ServiceNow

ServiceNow was started in 2004 with the belief that getting simple stuff done at work can be easy, and getting complex multi-step tasks completed can be painless. From the beginning, ServiceNow envisioned a world where anyone could create powerful workflows to get enterprise work done. Today, ServiceNow's cloud-based platform simplifies the way we work through a structured security response engine. ServiceNow Security Operations automates, predicts, digitizes, and optimizes security and vulnerability response to resolve threats quickly based on business impact. Reduce manual processes and increase efficiency across security and IT teams. ServiceNow is how work gets done. Learn more at servicenow.com.

Combined Solution



The diagram above shows the relationship between the Tenable Suite of ServiceNow Apps for Vulnerability Response, Ticketing (ITSM), Asset Tracking (CMDB) and the Tenable Connector.



Vulnerable Item
VIT0312647

Number: VIT0312647
Source: Tenable.io
Risk rating: 3 - Medium
Risk score: 40
Vulnerability: TEN-122784
Configuration item: epo59
State: Open
Assignment group:
Assigned to:
Created: 2019-12-16 15:49:49
Last opened: 2019-12-16
Updated: 2019-12-17 00:00:13

Summary: The remote Windows host is affected by multiple vulnerabilities.
Severity:
Vulnerability score (v3):
Vulnerability score (v2): 9.3
VPR Score: 9.5
Exploit exists: No
Exploit attack vector: -- None --
Exploit skill level: -- None --
Date published: 2019-03-12
Last modified: 2019-10-31
Threat: The remote Windows host is missing security update 4489883 or cumulative update 4489881. It is, therefore, affected by multiple vulnerabilities : - A remote code execution vulnerability exists when the

This image above shows a vulnerable asset within ServiceNow that contains vulnerability information such as risk rating, risk score and the Tenable Vulnerability Priority Rating (VPR).

More Information

You can get the latest apps here: store.servicenow.com

Installation and configuration documentation: docs.tenable.com

For support please visit: community.tenable.com

Watch Tenable Apps for ServiceNow — Value Overview on YouTube

Case Study — Fortune 500 Oil & Gas Company

tenable