

# Discovering, Assessing, and Remediating New Critical Vulnerabilities

A step-by-step guide to addressing new critical  
“named” vulns in InsightVM

## **TABLE OF CONTENTS**

---

<b>Introduction</b>	<b>3</b>
<b>Launching focused scans using scan templates</b>	<b>4</b>
<b>Reporting on affected assets with Dynamic Asset Groups</b>	<b>7</b>
<b>Visualizing affected assets with Live Dashboards</b>	<b>8</b>
<b>Creating Remediation Projects</b>	<b>9</b>
<b>Contact Us</b>	<b>11</b>

# Introduction

Dealing with new critical “named” vulnerabilities is nothing to new security teams.

Yet in recent years, vulnerabilities like Heartbleed and attacks like WannaCry have made international headlines, thrusting vulnerability management into the public spotlight.

When a new critical vulnerability or attack is discovered, others are probably asking you the following questions:

- How exposed are we to this attack?
- Have we already been compromised?
- What are we doing to mitigate this risk?

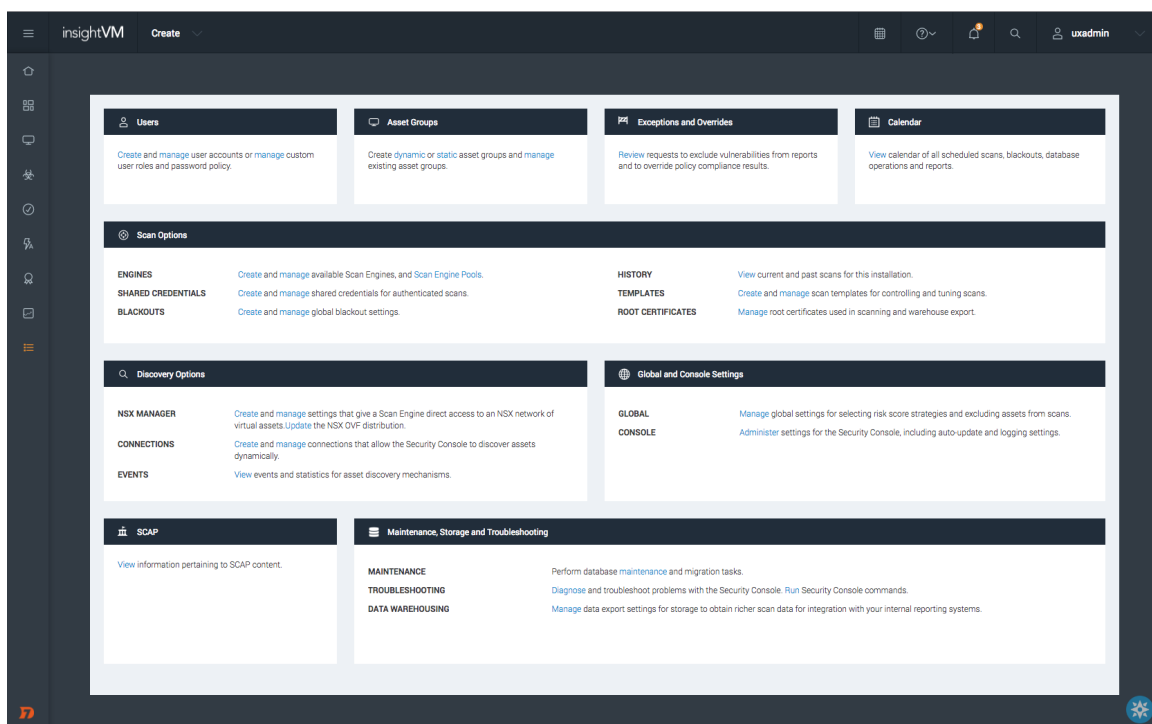
In this guide, we help you get a few steps closer to answering those questions by covering how InsightVM can:

- Launch a focused scan for a specific vulnerability or set of vulnerabilities
- Report on affected assets using dynamic filtering and Live Dashboards
- Streamline communications to help teams identify and address remediation activities

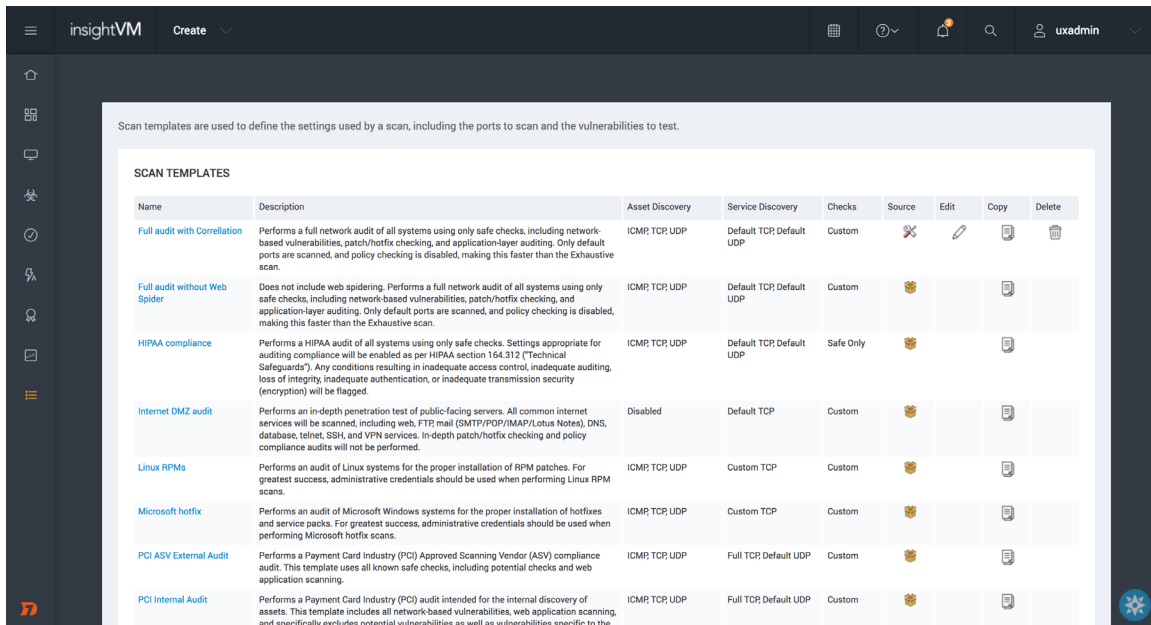
# Launching focused scans using scan templates

Scan templates in InsightVM dictate the mechanics of how scans are run. Although general audit scans cover new vulnerability checks as they're released, it's recommended that you create specific templates for critical vulnerabilities that are focused only on those relevant checks, as honed scans will run significantly faster.

## 1. Under the Administration tab, go to Templates, then select Manage Templates



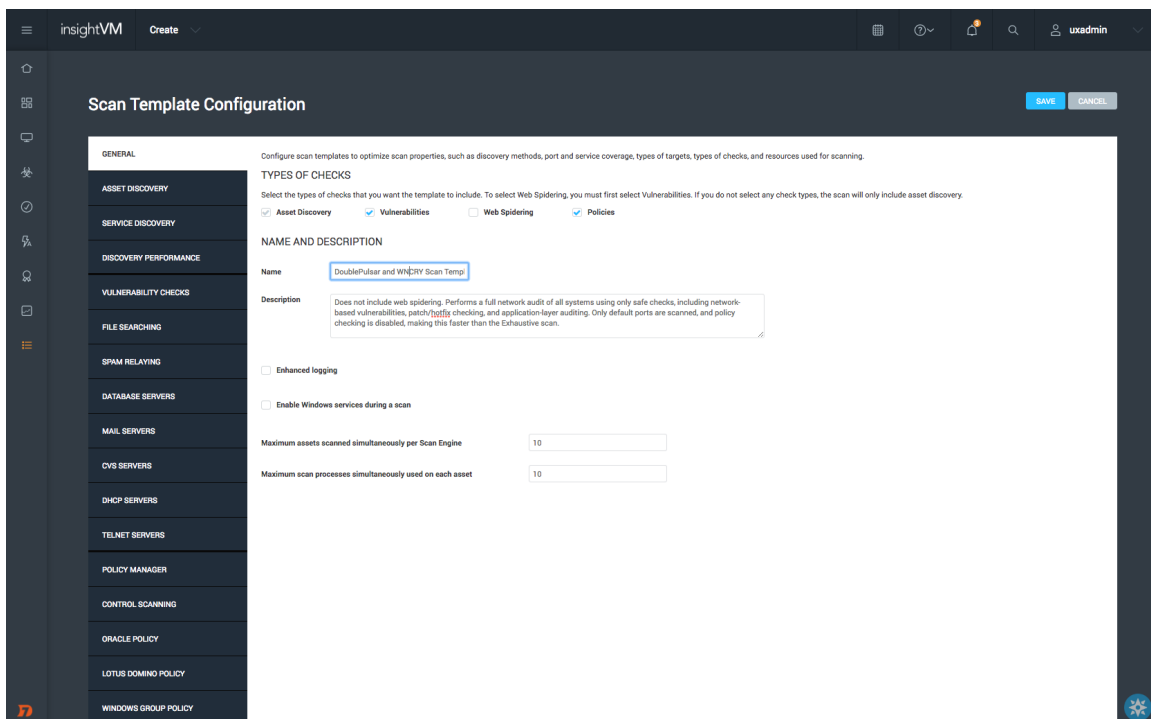
## 2. Copy the following template: “Full audit without Web Spider”



Scan templates are used to define the settings used by a scan, including the ports to scan and the vulnerabilities to test.

Name	Description	Asset Discovery	Service Discovery	Checks	Source	Edit	Copy	Delete
Full audit with Correlation	Performs a full network audit of all systems using only safe checks, including network-based vulnerabilities, patch/hotfix checking, and application-layer auditing. Only default ports are scanned, and policy checking is disabled, making this faster than the Exhaustive scan.	ICMP; TCP; UDP	Default TCP; Default UDP	Custom				
Full audit without Web Spider	Does not include web spidering. Performs a full network audit of all systems using only safe checks, including network-based vulnerabilities, patch/hotfix checking, and application-layer auditing. Only default ports are scanned, and policy checking is disabled, making this faster than the Exhaustive scan.	ICMP; TCP; UDP	Default TCP; Default UDP	Custom				
HIPAA compliance	Performs a HIPAA audit of all systems using only safe checks. Settings appropriate for auditing compliance will be enabled as per HIPAA section 164.312 ("Technical Safeguards"). Any conditions resulting in inadequate access control, inadequate auditing, loss of integrity, inadequate authentication, or inadequate transmission security (encryption) will be flagged.	ICMP; TCP; UDP	Default TCP; Default UDP	Safe Only				
Internet DMZ audit	Performs an in-depth penetration test of public-facing servers. All common internet services will be scanned, including web, FTP, mail (SMTP/POP/IMAP/Lotus Notes), DNS, database, telnet, SSH, and VPN services. In-depth patch/hotfix checking and policy compliance audits will not be performed.	Disabled	Default TCP	Custom				
Linux RPMs	Performs an audit of Linux systems for the proper installation of RPM patches. For greatest success, administrative credentials should be used when performing Linux RPM scans.	ICMP; TCP; UDP	Custom TCP	Custom				
Microsoft hotfix	Performs an audit of Microsoft Windows systems for the proper installation of hotfixes and service packs. For greatest success, administrative credentials should be used when performing Microsoft hotfix scans.	ICMP; TCP; UDP	Custom TCP	Custom				
PCI ASV External Audit	Performs a Payment Card Industry (PCI) Approved Scanning Vendor (ASV) compliance audit. This template uses all known safe checks, including potential checks and web application scanning.	ICMP; TCP; UDP	Full TCP; Default UDP	Custom				
PCI Internal Audit	Performs a Payment Card Industry (PCI) audit intended for the internal discovery of assets. This template includes all network-based vulnerabilities, web application scanning, and specifically excludes potential vulnerabilities as well as vulnerabilities specific to the	ICMP; TCP; UDP	Full TCP; Default UDP	Custom				

Don't forget to give your copy a name and description. In this example, we'll name our template “Double Pulsar and WNCRY Scan Template.”



Scan Template Configuration

GENERAL

Configure scan templates to optimize scan properties, such as discovery methods, port and service coverage, types of targets, types of checks, and resources used for scanning.

TYPES OF CHECKS

Select the types of checks that you want the template to include. To select Web Spidering, you must first select Vulnerabilities. If you do not select any check types, the scan will only include asset discovery.

☒ Asset Discovery ☒ Vulnerabilities ☐ Web Spidering ☒ Policies

NAME AND DESCRIPTION

Name: DoublePulsar and WNCRY Scan Template

Description: Does not include web spidering. Performs a full network audit of all systems using only safe checks, including network-based vulnerabilities, patch/hotfix checking, and application-layer auditing. Only default ports are scanned, and policy checking is disabled, making this faster than the Exhaustive scan.

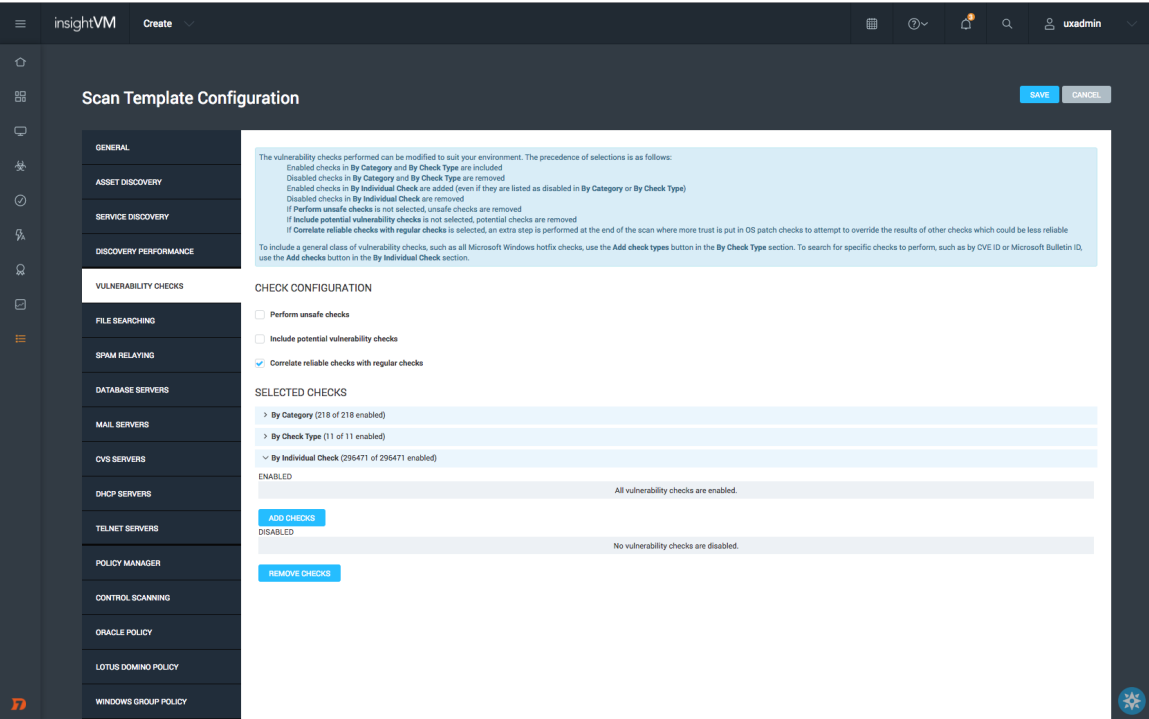
☐ Enhanced logging

☐ Enable Windows services during a scan

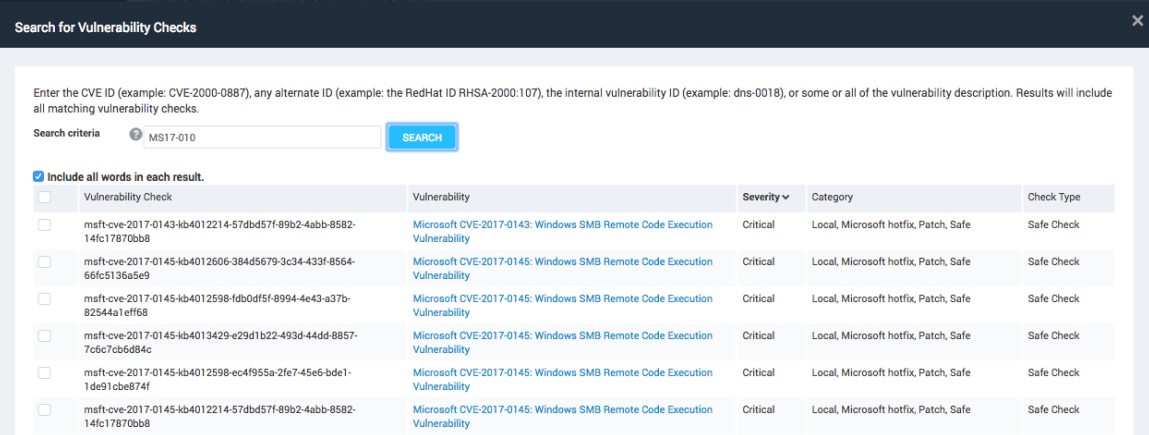
Maximum assets scanned simultaneously per Scan Engine: 10

Maximum scan processes simultaneously used on each asset: 10

3. Click on Vulnerability Checks, then By Individual Check.



4. Add in the specific CVEs or vulnerabilities you are scanning for and click save. In this example, we used “MS17-010”; you can also use individual CVEs.

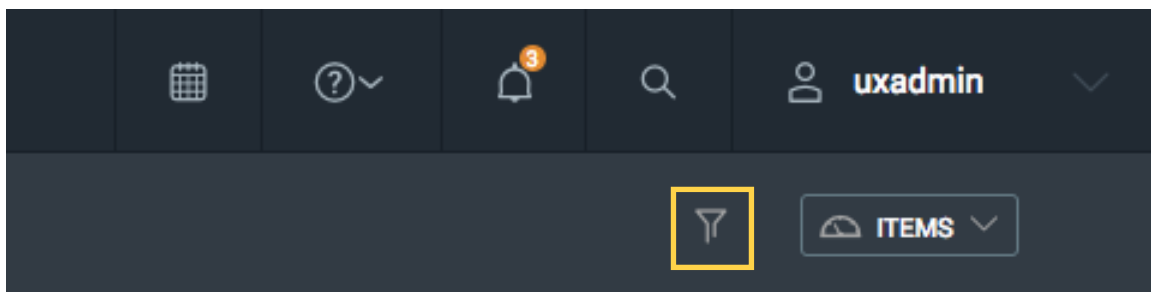


5. Save the template and run a scan to identify all assets affected by those vulnerabilities.

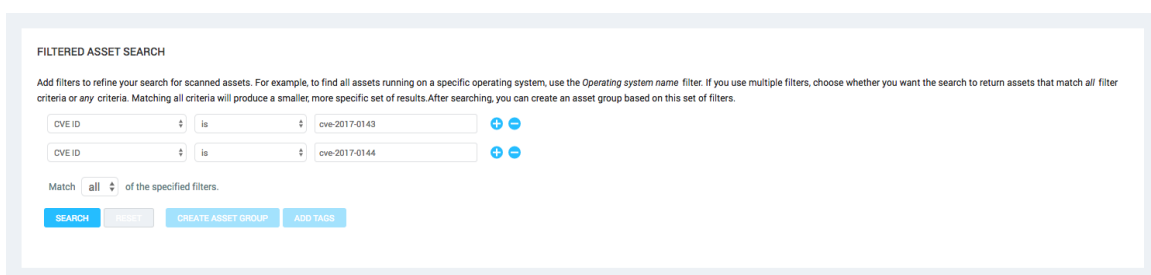
# Reporting on affected assets with Dynamic Asset Groups

Once assets have been scanned, create a Dynamic Asset Group for reporting and tagging that will update whenever new assets affected by this vulnerability are found (and fixed).

1. Click on the filter icon in the upper right corner of the InsightVM console, just under the search button.



2. Use the CVE ID filter to specify the which CVEs apply to you. For example, “CVE-2017-0143” and “CVE-2017-0144.”

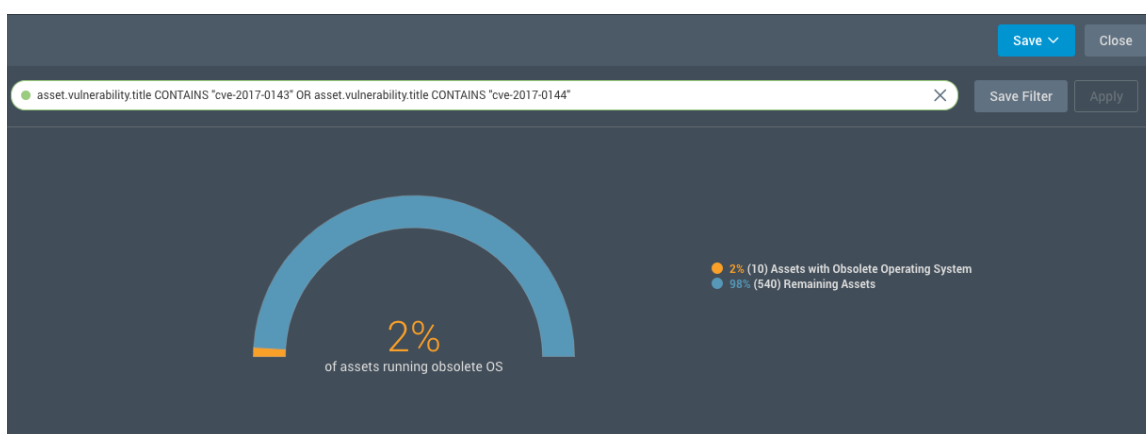


This asset group can now be used for reporting and tagging to quickly identify exposed systems.

# Visualizing affected assets with Live Dashboards

Live Dashboards in InsightVM can be customized with various cards on specific topics and trends, and most cards can be filtered down by simple query language. These filters scope dashboard cards down to the specific assets that are affected by a critical vulnerability. Use the filter “asset.vulnerability.title” to specify the appropriate vulnerabilities.

In the example below, we use “CVE-2017-0143” and “CVE 2017-0144” and filter using the following: asset.vulnerability.title CONTAINS “cve-2017-0143” OR asset.vulnerability.title CONTAINS “cve-2017-0144”<sup>1</sup>



<sup>1</sup> Note: You can use either “asset.vulnerability.title” or “vulnerability.alternateids” for these commands; the latter is useful for groups of vulnerabilities like Microsoft advisories on the format MS17-010, while the former is useful for specific vulnerability titles or CVEs.



# Creating Remediation Projects

Once you identify your exposure to a critical vulnerability, you want to ensure it's fixed as rapidly as possible across your entire network. Remediation Projects in InsightVM let you quickly send remediation steps to the specific team members responsible for affected systems, and track their progress in real time to patch vulnerabilities in a timely manner.

## 1. Go to the Projects tab and click Create a Project.

Project Name	Progress	Solutions Resolved	Remaining Time	Due On	% Assets Done	Assignees	Type	Status	Ticketing
Asset Group Project - Windows 8	0%	0 of 0	20 days	Wed, Sept 12, 2017	-	Conor, Admin	Static	Open	-
Assets with Expiring SSL Certs	84%	5803 of 6903	4 days	Thursday Aug 28, ...	0% (0 of 7)	Jillou	Static	Open	-
Assigned to Joe Smith	13%	132 of 1047	10 days	Mon, Sept 4, 2017	1% (0 of 1124)	Admin, Joe	Dynamic	Open	-
Austin Site Project	19%	42 of 219	6 days	Sat, Sept 1, 2017	0% (0 of 63)	Joe	Dynamic	Open	-
Boston Site - Assets Compliance	3%	668 of 26122	-	-	0% (15 of 4163)	-	Dynamic	Open	-
DISA related	0%	0 of 1	-	-	0% (0 of 2)	-	Dynamic	Open	-
FDCC Compliance - Austin Site	0%	0 of 0	-	-	-	-	Static	Open	-
IT FDCC Project	0%	0 of 64	-	-	0% (0 of 6)	-	Dynamic	Open	-
IT priority	12%	4 of 34	-	-	0% (0 of 1)	-	Dynamic	Open	-
Group A (Small) - Assets with Easy to Exploit Vulns	12%	4 of 34	-	-	0% (0 of 1)	-	Dynamic	Open	-
Legacy Issues - Patch Tuesday - July 2017	12%	4 of 34	-	-	0% (0 of 1)	-	Dynamic	Open	-
Patch Tues Priority - 2	0%	0 of 3	-	-	0% (0 of 2)	-	Dynamic	Open	-
Patch Tuesday	0%	0 of 3	-	-	0% (0 of 2)	-	Dynamic	Open	-
Riskiest Assets - High Priority	0%	0 of 34	-	-	0% (0 of 1)	-	Dynamic	Open	-
Riskiest Sites	0%	0 of 34	-	-	0% (0 of 1)	-	Dynamic	Open	-
Win 7 Enterprise SP1 Dynamic Remediations	0%	0 of 34	-	-	0% (0 of 1)	-	Dynamic	Open	-

2. Name the project, and use the following format for your filter: “vulnerability.alternatelds”. In the example below, we use “MS17-010”; you can also use individual CVEs.

The screenshot shows the 'Create Remediation Project' dialog box. The 'Name' field is filled with 'MS17-010 WannaCry/DoublePulsar Remediations'. Under 'Project Content', there are two filters: 'Asset filter' with '1251 Assets' and 'Vulnerability filter' with '6 Vulnerabilities'. The vulnerability filter is expanded, showing the filter expression 'vulnerability.alternatelds <=> ( altId = "ms17-010" )'. Below the filters is an 'Assign To' dropdown menu set to 'Select...'. There is a large 'Description' text area. At the bottom, there is a 'Due On' date field, an 'Access' section with checkboxes for 'Host Name', 'IP Address', and 'Operating System', and an 'Automated ticketing' section with a 'Not Configured' status and a 'Configure' button.

3. Give the project a description, configure who is responsible for remediation, and set appropriate access levels.

If you use Jira Software or ServiceNow ITSM, you can also configure the automatic ticketing integration between InsightVM and Jira or ServiceNow to automatically assign tickets to the right people. This project will update automatically as vulnerabilities get fixed, or as newly vulnerable devices are discovered.

Using these steps, you'll be able to easily assess, prioritize, and remediate any new critical vulns that come up.

Check out [blog.rapid7.com](https://blog.rapid7.com) for the latest threat analyses and advisories.

To get started for free, visit [rapid7.com/try/insightVM](https://rapid7.com/try/insightVM).

# About Rapid7

Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. Customers around the globe rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations. For more information, visit [our website](#), check out [our blog](#), or follow us [on Twitter](#).

