**TP ICAP**  
**Information Technology: Platform Services**  
  
  
**Patching Qualys Checks**  
**Version 1.0**

**TP ICAP Classification:** **Internal**  
  
  
  
**Document History**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Description** | **Who** | **Reviewed** | **Location** |
| 1.0 |  | Dennis Jeffrey Flores |  | Manila, Philippines |

**Document Owner**

|  |  |  |
| --- | --- | --- |
| **Name** | **Job title** | **Team** |
| Harjot Kandola | Global Head Wintel Operations | Wintel |

**Author/Contributors**  
This version of the document was written and approved by

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Name** | **Job title** | **Sections** | **Date** | **Evidence of Approval** |
| **Author** | Dennis Jeffrey Flores | Wintel Team Lead | Complete document | 5/24/2023 | EMAIL |
| **Contributors** |  |  |  |  |  |
| **Review** | Harjot Kandola | Global Head of Wintel Support |  |  | EMAIL |
| **Other reviewers** |  |  |  |  |  |
| **Approved Granted by** | Harjot Kandola | Global Head of Wintel Support |  |  |  |

**Review Period**

|  |  |
| --- | --- |
| **Review Period / Cycle (months)** | **Next Review Date** |
| 12 months | May 2024 |

**Distribution List**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Function** | **Date of Issue** | **Date reviewed** |
| Wintel Operations | Wintel Operations |  |  |

**Document Security:** **Internal**

**Introduction**

Patching is critical for fixing software vulnerabilities. It's equally important to confirm these patches are successful. We use Qualys, a third-party tool, to scan for vulnerabilities and verify our patching efforts. This allows us to identify and address any remaining server vulnerabilities after a patching cycle. Through this process, we uphold our commitment to the highest level of security.

**Document Summary:**

This document outlines securing security scans from infosec using Qualys against previously patched servers.

**Scope**

The scope of this document covers windows patching cycle

Background

|  |
| --- |
| **What does this process do?** |
| Provide documentation on how to request Qualys scans to validate a patch cycle activity |
| **What does this Service do?** |
| Validate Patching Cycle Success Rate |
| **Which area of the company does this apply to?** |
| Wintel Engineer team performed the patching cycle. |
| **When should / could this Service be used?** |
| Right after the patching cycle |
| **When should it not be used?** |
| Not applicable to individual server patching activities or vulnerability remediation. Please remember that this document's scope describes how to measure the success rate of the previous patching cycle via Qualys and not to remediate server vulnerabilities. |

**Procedures**

During every patching cycle, the change manager will send two server lists: a provisional and a final list of servers targeted for the upcoming patching cycle. The final list of servers needs to be submitted to Infosec using the following ServiceNow link:

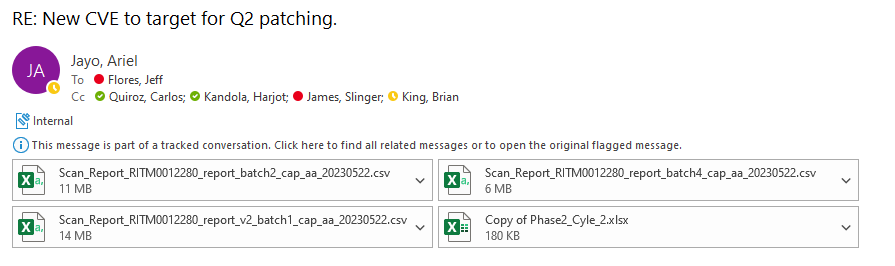
[Vulnerability Management Requests - TPICAP Service Portal (service-now.com)](https://tpicap.service-now.com/tpicap_sp?id=sc_cat_item&sys_id=8a5f34fa1b36955001cf8591f54bcba0&sysparm_category=6fc093da1b7ca11001cf8591f54bcb2c)

Please submit the final spreadsheet for vulnerabilities with severity five (5) and request the job to be run starting Sunday at 4:00 am, Singapore time.

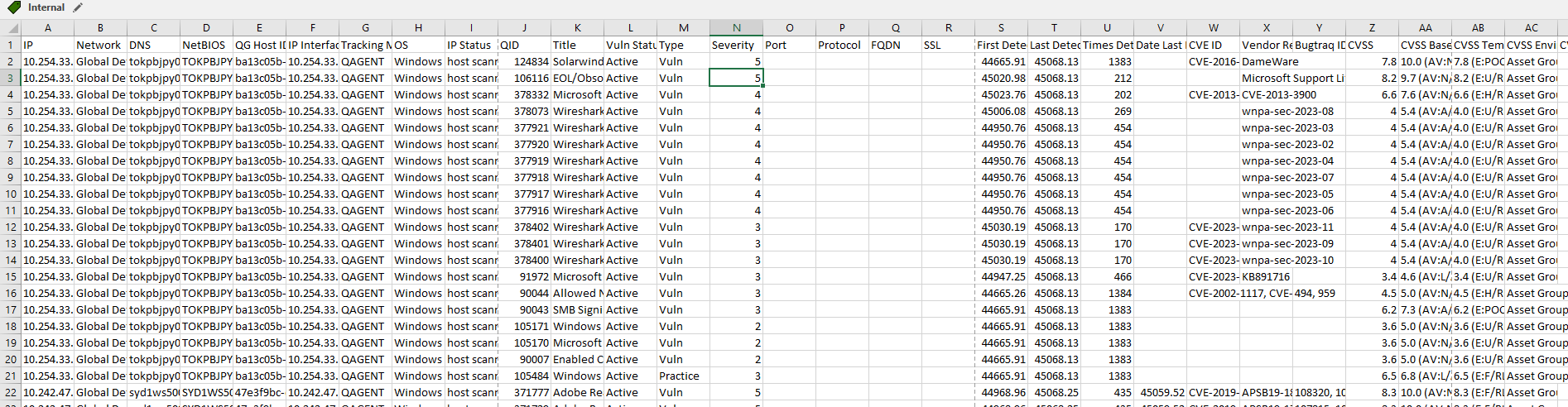
Please notify the following distro of the ticket number, the list, and the schedule.

Global IT Security [GlobalITSecurity@tpicap.com](mailto:GlobalITSecurity@tpicap.com)

TP ICAP Global Wintel Administrators [WintelAdministrators@tpicap.com](mailto:WintelAdministrators@tpicap.com)

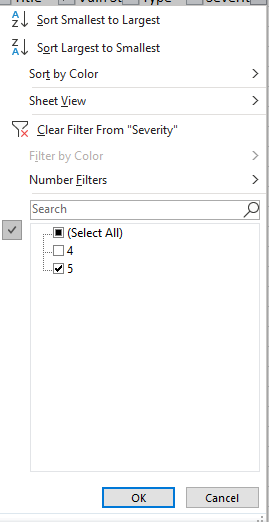


The vulnerabilities need to be dump in a single file like so:

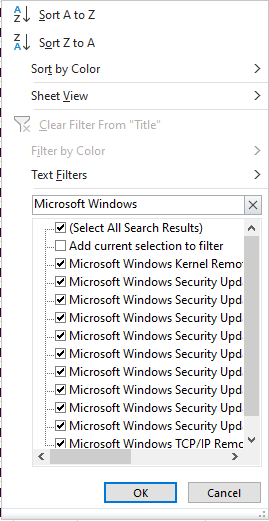


The following filter needs to be applied to determine Wintel Owned Vulnerabilities:

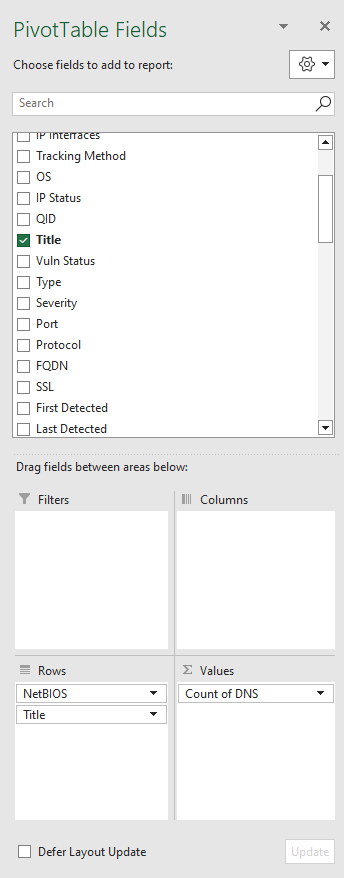
Severity 4 and 5:



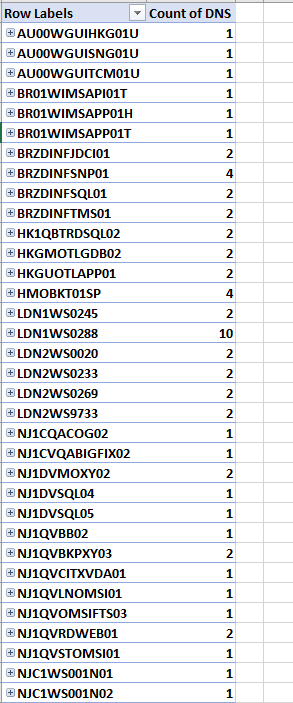
Title: Filter for text containing Microsoft Windows.



From The resulting data, create a pivot table with the following filters:



You will get a list of servers that contains vulnerabilities with severity five (5). These servers must be remediated on the next patching cycle or through an ad-hoc change. You have identified the list of servers that did not fully apply the latest patch from the patching cycle.



Send the results to the Windows team and line up resources for remediation

TP ICAP Global Wintel Administrators [WintelAdministrators@tpicap.com](mailto:WintelAdministrators@tpicap.com)

To get the success rate, the number of unique servers from you final list