How to: Patch a Server

Exported on 11/14/2022

Table of Contents

No headings included in this document

Purpose

Qualys gives us a new vulnerability report each week, which gives us new updates to install. Some of these updates do not install by themselves and will require human intervention. Some examples would be if an install failed or requires the server to be reset to take effect. You will need to go through the process of figuring out what patches you will need to apply manually, finding the servers that need to be patched, and applying the patch.

Prerequisites

You will need:

- RA account
- Power BI
- Access to Qualys weekly report

Process

1. Open Power BI
2. Find the Qualys report in path: \
   \alawpokcarc200\Departments\Development\VulnerabilityReports\QualyScanPowerBi(Other)

Name	Date modified	Type	Size
NetSparkerReport.twb	5/18/2020 6:56 PM	TWB File	246 KB
QualyScanPowerBi(IPFC)	7/21/2022 1:13 PM	Microsoft.MicrosoftP...	5,996 KB
QualyScanPowerBi(Other)	7/21/2022 1:13 PM	Microsoft.MicrosoftP...	6,009 KB
QualyScanPowerBi	6/30/2022 8:10 AM	Microsoft.MicrosoftP...	5,822 KB
QualysScans.twb	4/20/2021 8:36 AM	TWB File	1,285 KB

3. Check the severity 3 and 4 tabs for vulnerabilities with a very small IP count

Windows Digital Signatures Remote Code Execution Vulnerability (MS13-098)	2
Microsoft Windows Network File System (NFS) Remote Code Execution (RCE) Vulnerability...	1
Microsoft Windows Network File System (NFS) Security Update for July 2022	1

4. Open SQL Server Management Studio
5. Connect to ALAWNOKCSQL302
6. Run the below query to check the patch names and which servers need to be patched:

    SELECT DNS, NetBIOS, OS, Title, Solution, Results, [First Detected], DATEDIFF(DD, [First Detected], GETDATE()) AS [Age], [CVE ID], SPP.Phase, D.QID, D.Severity
    FROM VulnerabilityReports.dbo.DailyQualysScans D

LEFT JOIN VulnerabilityReports.dbo.ServerPatchPhases AS SPP (NOLOCK)
ON (SPP.ServerName = D.NetBIOS OR SPP.ServerName = D.DNS)
WHERE DateLoaded >= '7/18/2022' --AND DateLoaded < '4/18/2022'
--AND D.QID = '90080'
--AND D.NetBIOS IN ('ALAWPWCOMFS100','BCTWPECOSQL300')
--AND SPP.Phase = 1
--ORDER BY D.Title, D.NetBIOS
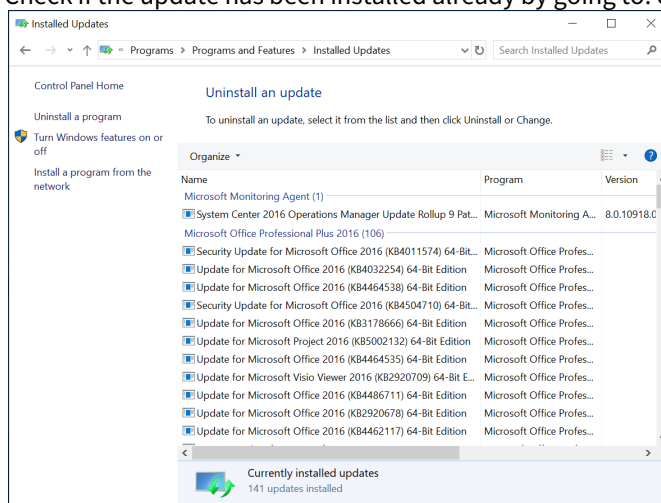--AND D.dns LIKE '%web203%'
AND Title LIKE '%%'

(Enter a keyword between the % signs. EX: Office)

7. RDP into the server that needs the patch
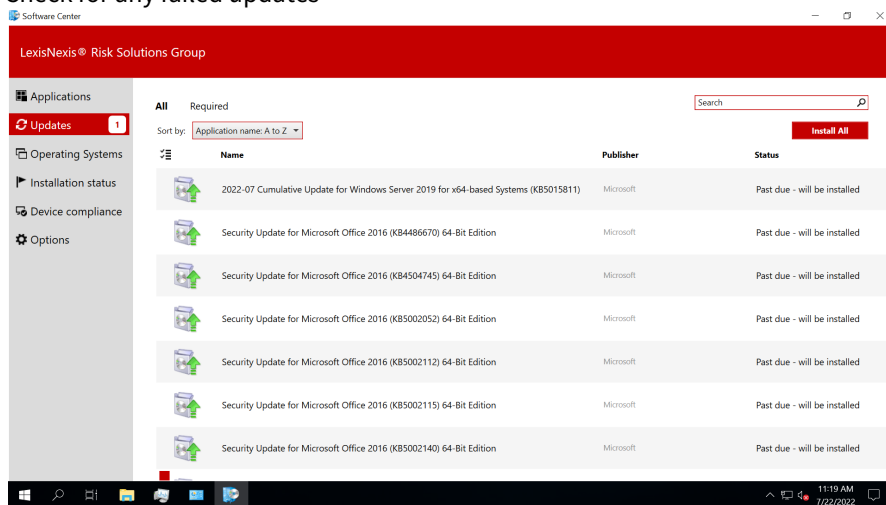8. Open file explorer and check disk space
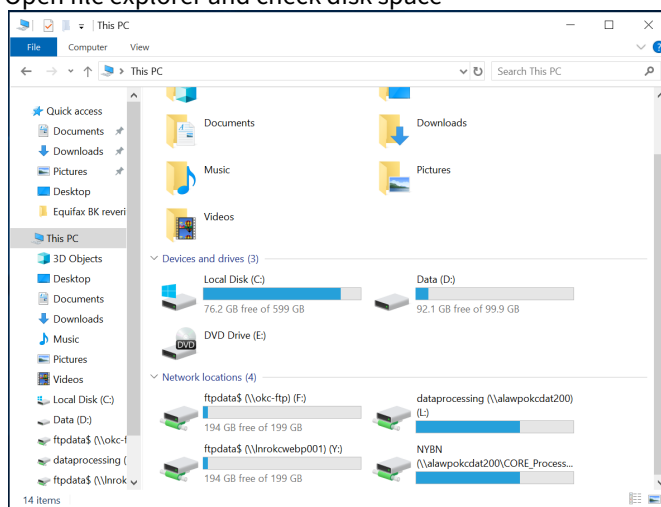
9. Go to C: > Utils > DiskCleanUp and EmptyAllRecycleBins if disk space is full
10. Check if the update has been installed already by going to: control panel > installed updates

11. Go to software center > updates

12. Check for any failed updates

13. If an update says "waiting to be installed", then there are no further steps to take
14. If an update is not in the queue, search for the update in the browser

Caution

If the server requires a reboot to install, consult the owner of the server for permission before proceeding. The owner of the server can be found by going to CDB portal (CDB Portal - Index (lexisnexis.net)[1]), then enter the server name into the search bar. Go to the "app support" tab, then navigate to the application contacts section.

---

1 https://cdb.rs.lexisnexis.net/index.php