Guardicore

# Mitigating May 2019 Patch Tuesday Vulnerabilities with Guardicore Centra

Vulnerability Alert

# Mitigating May 2019 Patch Tuesday Vulnerabilities with Guardicore Centra

May 2019 Patch Tuesday consists of multiple critical vulnerabilities affecting large organisations. Among the vulnerabilities disclosed were two possibly 'wormable' vulnerabilities in Windows systems, which Microsoft has decided to patch way down to out-of-support Windows XP and Server 2003 versions. Other notable vulnerabilities reported on Microsoft patch Tuesday include two vulnerabilities that allow complete compromise of many Cisco network devices and a flaw in Citrix Workspace that allows attackers to steal data from endpoint machines running Citrix software.

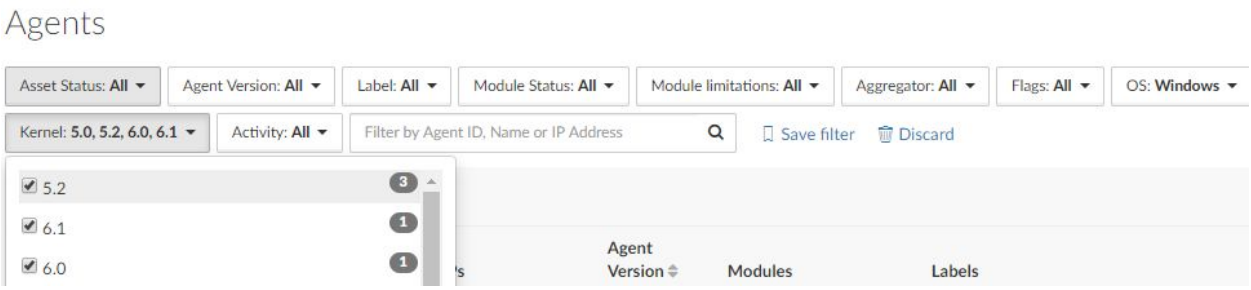
In this post we're providing Guardicore customers advice on how to detect and mitigate the vulnerabilities we consider crucial for data center security. Guardicore Centra's Agents cover all Microsoft Windows versions from Windows XP through Windows Server 2019. To be able to detect vulnerabilities and reduce attack surface, we recommend deploying Agents throughout your entire data center. For more information about Patch Tuesday vulnerabilities read our post published yesterday.

## Microsoft's Remote Desktop Services - CVE-2019-0708

This is a potentially 'wormable' vulnerability in the Windows Remote Desktop Service. A successful exploit will provide attackers with full control of the victim server without the need for any valid credentials. Using Centra, it is possible to detect vulnerable Windows Server machines and mitigate risk.

### Detection

To find vulnerable machines, from **Administration** go to **Components** >**Agents**, and filter by operating systems to display only Windows machines with the following kernel versions - 5.1, 5.2, 6.0, 6.1.

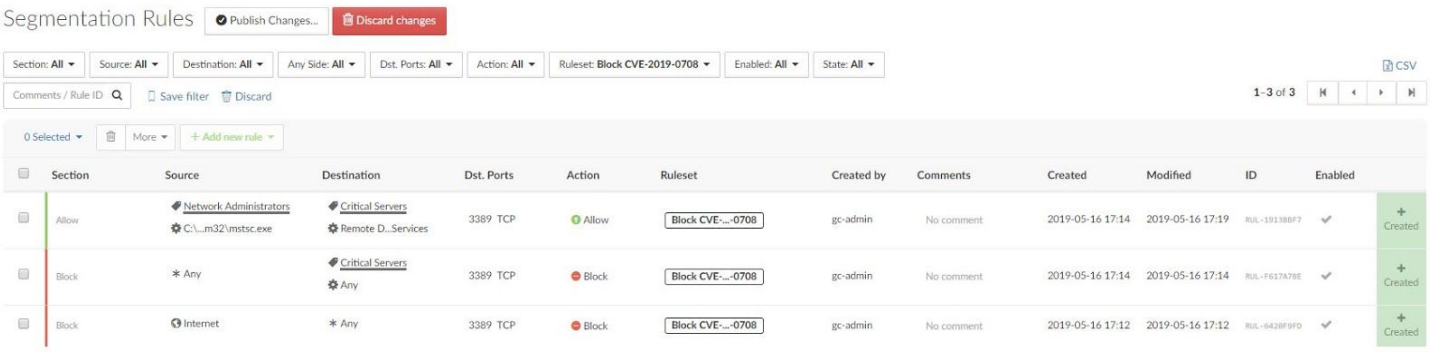



These machines run a vulnerable version of Windows and should be patched.
Note, Guardicore Centra can help you detect vulnerable machines only when you have an Agent deployed.

## Mitigation

With Centra you can reduce your network's attack surface dramatically by blocking potentially malicious traffic. Create a Block rule for incoming traffic from any internet source to Windows remote desktop service (TCP port 3389). If you have any known exceptions to this rule, create an Allow rule to whitelist these exceptions (preferably with specific sources and destinations).

You can also use Centra to limit internal access to critical servers, which will reduce the potential wormable factor of this vulnerability.



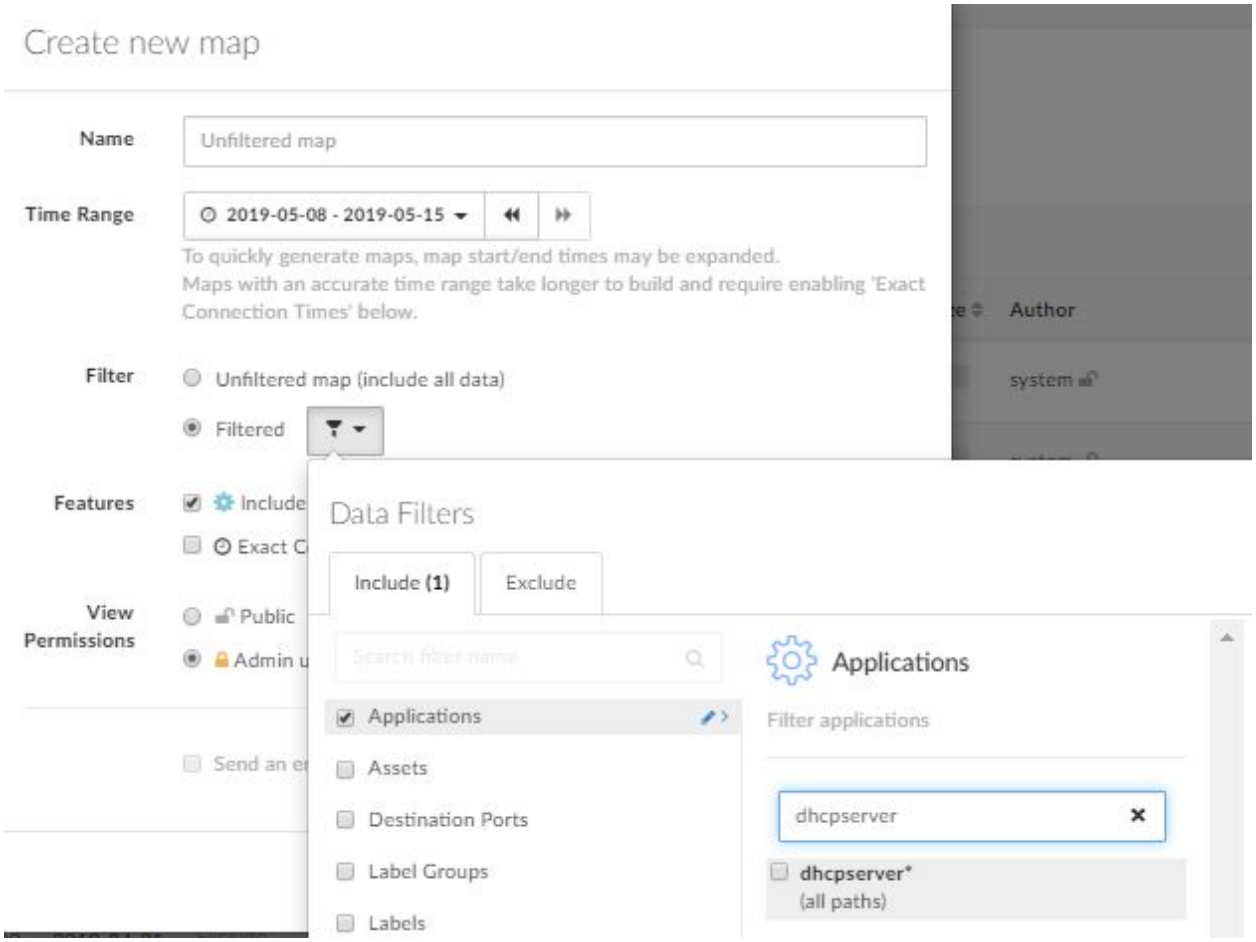
# Microsoft DHCP Server - CVE-2019-0725

This vulnerability is a remote code execution flaw in Microsoft's DHCP Server. A successful compromise of a DHCP server allows attackers to take over the addressing schema used in the network and potentially inject malicious data into the organisation's DNS servers. From there, it is typically a matter of time till attackers have full control over the network.

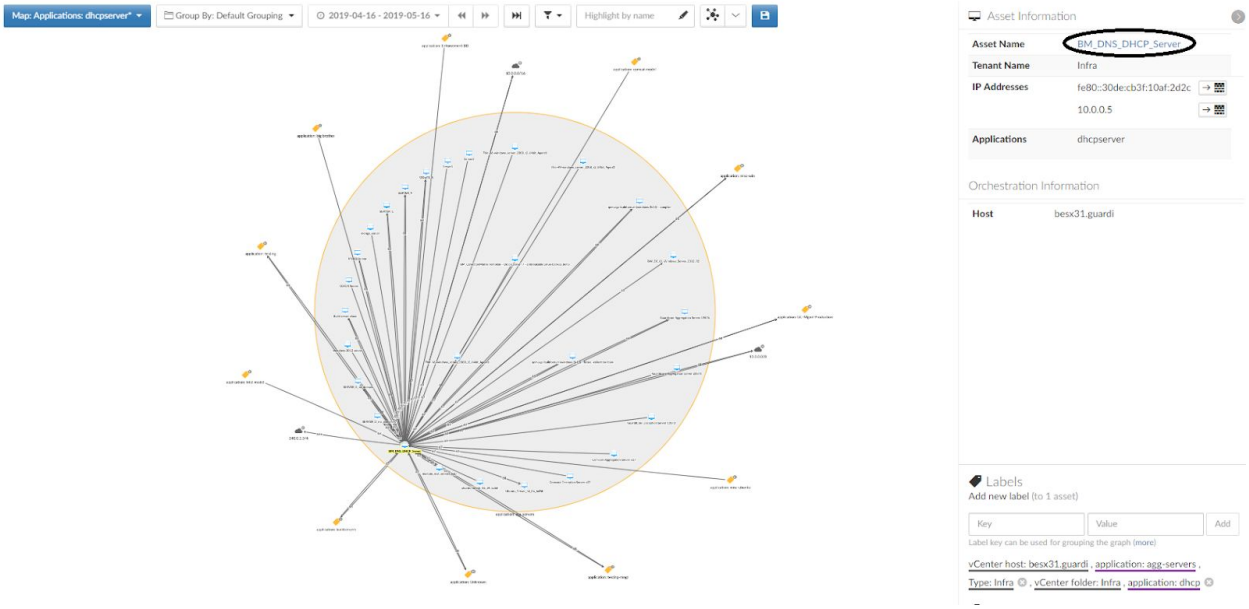
## Detection

You can use Centra to find vulnerable assets in your network.
From **Reveal,** go to **Saved Maps**, click **Create New Map** and set the following conditions:

- In time range select "Last 7 days"
- Filter the map by Applications and search for "dhcpserver". Click **Apply**.



For each of the DHCP servers on the map, check if one of the processes in the servers is "dhcpserver". Once you've identified the assets running a DHCP server, you can open their asset page from the map's Asset Information pane.




Clicking **Asset Name** opens the asset page and displays the operating system of the asset. If the operating system is one of the following the server is vulnerable:

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2019

## Mitigation

Use Centra to reduce the attack surface by limiting access to the network's DHCP servers.

- Create an Alert / Block rule for any incoming DHCP traffic from the internet.
- Create an Alert / Block rule for DHCP communications between DHCP servers and subnets they shouldn't communicate with.

# Cisco's Routers (*Thrangrycat*) - CVE-2019-1649, CVE-2019-1862

Two vulnerabilities, one in the web administration interface and one in the secure boot process, allow an attacker to gain full control over Cisco hardware and through this potentially compromise the entire network.

## Mitigation

The risk posed by this vulnerability can be reduced using Guardicore Centra.
We suggest the following:
1. Label the machines or subnets used by your network administrators to work with Cisco routers, switches and other devices.
2. Create additional labels for management IP addresses of your Cisco routers, switches and other devices.
3. Once you have these labels in place create the following rules:
***Allow*** *"network administrators label" to "routers label" on any port*
***Alert*** *(or* ***Block****) any to "routers label" on any port*

These rules will generate alerts on traffic from unauthorized users to the routers, allowing you to detect possible attackers.