



Virtualization Vulnerabilities

VULNERABILITY MANAGEMENT

Virtualization Vulnerabilities

- VM Escape
- Management Interface Access
- Virtual Host Patching
- Virtual Guest Issues
- Virtual Network Issues



VM Escape

- Most serious of all virtualization issues
- Occurs when an attack can break out of the virtual machine (guest) and reach the host (hypervisor)
- In May 2017, a hacking contestant stitched together 3 different exploits and managed to perform a VM escape

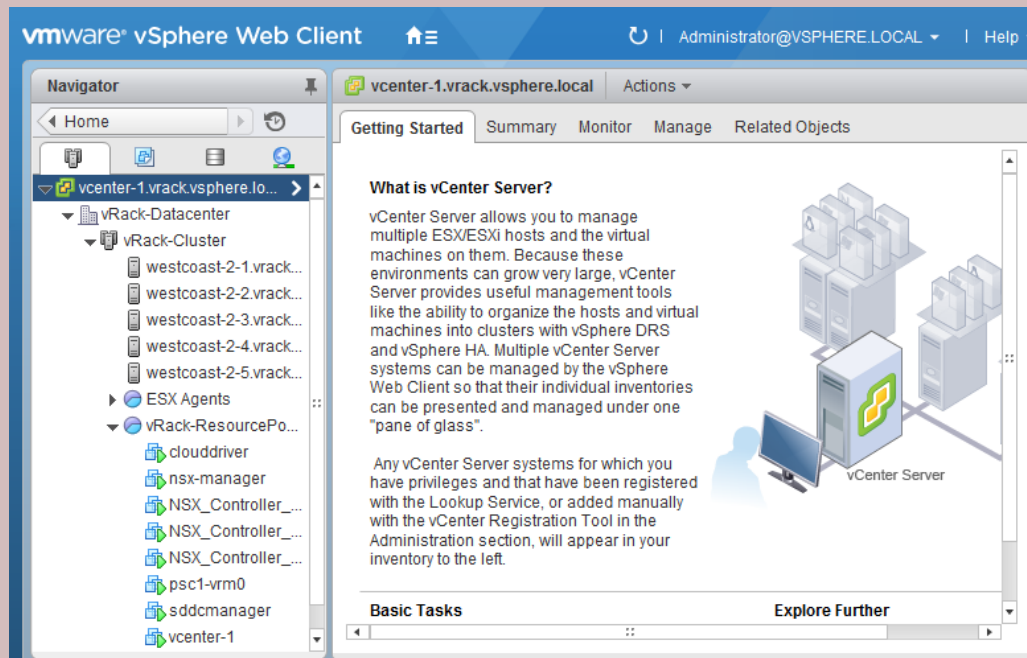
Source:

<https://arstechnica.com/information-technology/2017/03/hack-that-escapes-vm-by-exploiting-edge-browser-fetches-105000-at-pwn2own/>



Management Interface Access

- This interface controls access to all the virtual machines and can configure them
- Should be highly secured, including use of two-factor authentication



Virtual Host Patching

- Just like other servers Virtual hosts need patching of their OS and software
- This can help prevent VM Escape

File Edit View Inventory Administration Plug-ins Help

Home Solutions and Applications Update Manager pml-pod20-vc01 Search Inventory

Update Manager Administration for pml-pod20-vc01

Baselines and Groups Configuration Events Notifications Patch Repository ESXi Images VA Upgrades

Patch Name, Product, Release Date, Type, Severity, Category, Impact, Vendor or Patch ID contains: Advanced... Clear Import Patches Compliance V

Patch Name	Product	Release Date	Type	Severity	Category	Impact	Vendor	Patch ID	Baselines
Updates esx-base	embeddedEsx 5.0.0	12/15/2011 12:00...	Patch	Important	Security	Reboot	VMware, ...	ESXi500-...	Add to ba...
Updates tools-light	embeddedEsx 5.0.0	12/15/2011 12:00...	Patch	Important	BugFix		VMware, ...	ESXi500-...	Add to ba...
Updates net-e1000 and net-e1000e	embeddedEsx 5.0.0	12/15/2011 12:00...	Patch	Important	Security	Reboot, Mai...	VMware, ...	ESXi500-...	Add to ba...
Updates misc-drivers	embeddedEsx 5.0.0	12/15/2011 12:00...	Patch	Low	BugFix	Reboot	VMware, ...	ESXi500-...	Add to ba...
Updates net-be2net	embeddedEsx 5.0.0	12/15/2011 12:00...	Patch	Low	BugFix	Reboot, Mai...	VMware, ...	ESXi500-...	Add to ba...



Virtual Guest Issues

- Each guest represents another server on the network, and they all need patching
- Ensure your remediation and patch management considers all your VMs
- Ensure your vulnerability management program also scans Guest VMs



Virtual Network Issues

- Virtual firewalls, routers, and switches all need to be considered as part of your scanning program
- If embedded as part of your VM solution, ensure appropriate patching is being done to prevent attacks

