VMware NSX Data Center Flaw Can Expose Virtual Systems to Attacks

By Eduard Kovacs on February 18, 2022

Details of Recently Patched VMware NSX Vulnerability Disclosed

VMware this week announced the availability of a patch for a high-severity vulnerability affecting the NSX Data Center for vSphere network virtualization product.

The vulnerability is tracked as CVE-2022-22945 and it has a CVSS score of 8.8. VMware described it as a command-line interface (CLI) shell injection vulnerability affecting the product's NSX Edge appliance component. The flaw could allow a remote attacker to execute arbitrary operating system commands as root.

VMware patched the vulnerability in NSX Data Center for vSphere with the release of version 6.4.13. Cloud Foundation (NSX-V) is also impacted, but a fix has yet to be released.

Dimitri Di Cristofaro and Przemek Reszke of UK-based penetration testing firm SECFORCE have been credited for reporting the vulnerability to VMware. SECFORCE on Friday published a blog post detailing the vulnerability and its implications.

NSX Data Center for vSphere can be used to create, snapshot, delete and restore software-based virtual networks. The security hole was discovered by SECFORCE during a pentesting job targeting

VMware Cloud Director, a solution designed for managing large-scale cloud infrastructures.

CVE-2022-22945 affects the NSX Edge appliance component, which is a virtual router that sits on the edge of the tenant network and enables communication between virtual data centers and the outside world.

Users with administrative privileges can enable SSH on the NSX Edge router, which enables access to a restricted Linux shell that can be used to configure the router. This "jailed shell" only allows the execution of certain commands for network management.

The vulnerability patched this week can be exploited to escape this jailed shell and obtain a root shell on the underlying operating system. However, in order to exploit the flaw, an attacker needs SSH access to the targeted device and they also need valid credentials for any account on the device.

"It is not necessarily trivial to obtain these [credentials]. However, if weak / guessable credentials are in place or if the credentials are obtained via some other attack, the attack would be possible," SECFORCE explained.

According to SECFORCE, exploitation of CVE-2022-22945 could allow an attacker — in addition to gaining unrestricted access to the underlying operating system — to install malware on the virtual device, and gain unrestricted network access to virtual servers, including for network traffic capture and MitM attacks.

In addition to installing patches, SECFORCE has advised organizations to ensure that the SSH service running on the NSX Edge router is not exposed to the internet — access should be limited to trusted IP addresses if the device needs to be managed over the internet.

It's important that organizations do not ignore patches released by VMware as it's not uncommon for malicious actors to target the virtualization giant's products in their attacks.

Earlier this month, VMware patched several serious vulnerabilities disclosed last year by researchers at China's Tianfu Cup hacking contest.

Related: VMware Plugs Security Holes in Workstation, Fusion and ESXi

Related: VMware Patches Critical Flaw in Workspace ONE UEM Console

Related: VMware Confirms In-the-Wild Exploitation of vCenter Server Vulnerability

Eduard Kovacs (@EduardKovacs) is a contributing editor at SecurityWeek. He worked as a high school IT teacher for two years before starting a career in journalism as Softpedia's security news reporter. Eduard holds a bachelor's degree in industrial informatics and a master's degree in computer techniques applied in electrical engineering.

Previous Columns by Eduard Kovacs: