VMware Critical Patch Update

HHS 405(d) Program SBAR Brief

October 8, 2021

The 405(d) **S**ituation, **B**ackground, **A**ssessment, **R**ecommendation (SBAR) is an HPH focused review of active cyber intelligence and alerts from across federal agencies. Mandated by the Cybersecurity Act of 2015 with the goal of aligning industry security approaches, the 405(d) **SBARs**, backed with the knowledge and expertise of HHS and the 405(d) Task Group, provide the HPH sector with a clear HPH focused understanding, assessment, and recommended mitigations that HPH organizations can apply against these active cyber incidents.

A concise statement of the problem

SITUATION: On September 21, 2021 VMware, Inc informed the public of (19) vulnerabilities affecting their vCenter Server and cloud products. These products are used extensively in supporting the healthcare community. **The arbitrary file upload vulnerability is the most critical of the (19) vulnerabilities identified.** Arbitrary file upload has the potential to allow an unidentified person to ultimately run a backend script to gain access to your network and upload malicious files, thus gaining access to transfer sensitive data and potentially complete a system takeover. Due to the increased risk of a ransomware attack posed by this vulnerability, a patch has been released to mitigate this issue. With the increased cyber-attacks on critical infrastructures, such as the healthcare industry, critical security patches should be applied with urgency after a vulnerability has been identified to ensure your patients' data remains secure.

Pertinent and brief information related to the situation

BACKGROUND: System Administrators are the gatekeepers of any organization's computer's network. They are responsible for management, reliable operations, and support activities for all users on the network. They also have increased privileges that a traditional user would not have. Due to its elevated privileges, the administrator account has become a target for attackers. This access would allow attackers to change settings, edit files, initiate a ransomware attack, or worse. This could result in a complete shutdown of the computer's network. Therefore, the arbitrary file upload vulnerability currently affecting the VMware vCenter Server should be addressed immediately. The arbitrary file upload vulnerability allows execution of software that may make it easier for attackers to compromise other systems and the ability to plant malicious software on the affected network. Additionally, this vulnerability also affects VMware's cloud computing technology. With so many small to medium healthcare organizations turning to cloud technology as a more secure security solution to protect their patients' PHI information, it is important to remember that they are not immune to a possible ransomware attack. So, it is becoming increasingly important to stay vigilant to these types of vulnerabilities.

Analysis and considerations of options—what we found and think

ASSESSMENT: The arbitrary file upload vulnerability found in the vCenter servers grants access to any attacker without authenticating them prior to granting access to the network. This is a high risk and does not follow the zero-trust model which requires organizations to verify the identity of all users that access their network. Also, many of the applications installed on medical devices are connected to the Internet. This risk can also affect the Internet as an attacker can inject code onto a website or link which, once clicked on, would grant access to the person's network. VMware states that this vulnerability exists "regardless of the configuration settings" which, in-turn, makes the vulnerability the default and undetectable to the system administrators.[1]

Recommended/ requested action—what we want you to do

RECOMMENDATION: It is recommended that you talk with your IT security team and contractors to ensure all your systems are being patched. It is also recommended that you implement a good patch management process. "At least monthly, organizations should implement patches that are produced by the vendor community. IT operations should collect these patches, conduct appropriate regression tests to ensure that patches do not negatively impact the business, and schedule patch implementation during routine change windows. This process should be executed and measured using standard IT operations activities."[3]

You should also stay connected to organizations that can notify you about new patches when they are released. Your organization's IT security team should stay up to date on the current vulnerabilities affecting your sector. "The National Vulnerability Database (NVD) has produced the CVSS, a standard measurement across all industries that normalizes and ranks the severity of a vulnerability."[3]

It is also recommended that your organization establishes a patch management process. "All organizations should have a routine to patch security flaws in their servers, applications (including web applications), and third-party software. Although the patching process may vary, large organizations should use centralized systems to interrogate servers and determine which software updates should be implemented."[3] You can find this and other helpful patch management tools in the HICP publication Technical Volumes #1 and #2 under "Patch Management."[2, 3]

Additional Resources:

VMware Security Advisory

HC3 Sector Alert: VMware

Sources:

1. Plug critical VMware vCenter Server flaw before ransomware gangs start exploiting it (CVE-2021-22005)
2. HICP Technical Volume 1: Cybersecurity Practices for Small Health Care Organizations
3. HICP Technical Volume 2: Cybersecurity Practices for Medium and Large Health Care Organizations