lightstream

Lightstream Cyber Security

Flash Bulletin | May 18, 2022

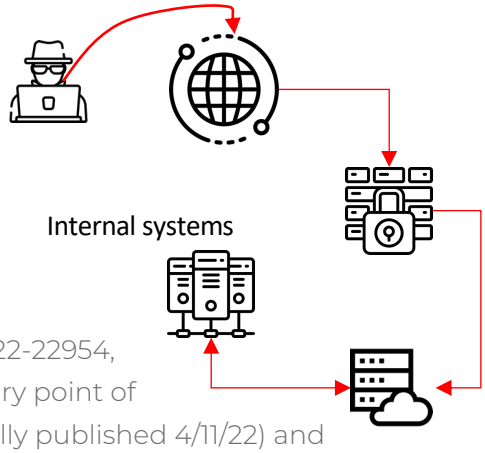
VMWare Infrastructure Actively Exploited to Compromise Organizations

CISA, the Cybersecurity and Infrastructure Security Agency, has issued an emergency directive highlighting an escalation of successful attacks against commonly deployed enterprise components of VMWare virtual infrastructure. The directive points to an escalation of **successful attack** against a series of VMWare vulnerabilities that are exploited independently, or in combination, to **fully compromise VMWare infrastructure** in these organizations. While VMWare has issued patches for these vulnerabilities, attackers have quickly reverse engineered them to develop and weaponize exploits now appearing in the wild.

The attacks highlighted require network access, but successful attackers have utilized 3rd party network access and web exposed servers to compromise vulnerable VMWare components and gain full access.

Business Impact

Exploitation of this set of vulnerabilities gives attackers **complete control** over the VMWare virtual infrastructure. This means that critical business systems can be manipulated, destroyed, or silently monitored by attackers. If your organization depends on VMWare components highlighted below your business is likely at risk of compromise.



Security Impact

The CVE numbers for the critically impacted vulnerabilities are CVE-2022-22954, CVE-2022-22960, CVE-2022-22972, CVE-2022-22973; however, the primary point of attack has been CVE-2022-22954 which has a CVSS score of 9.8 (originally published 4/11/22) and results in a potential Remote Code Execution (RCE). It is recommended that any exposed components to the Internet **should be assumed compromised** and disconnected/investigated immediately. VMWare customers should also immediately deploy additional monitoring of their VMWare infrastructure and monitor for IOCs.

Urgent Actions Required

1. Identify VMWare Workspace ONE Access and Identity Manager infrastructure, scan for vulnerabilities
2. Disconnect/investigate infrastructure with missing patches exposed to the Internet, or 3rd party access
3. Urgently apply missing patches described above in VMWare infrastructure, monitor for compromise

Recommendations

The vulnerabilities are present in the following VMWare components: VMware Workspace ONE Access (Access), VMware Identity Manager (vIDM), VMware vRealize Automation (vRA), VMware Cloud Foundation, and vRealize Suite Lifecycle Manager. These should be placed under heightened security monitoring, patches urgently applied (if not already done) and threat hunt activity should be initiated using the available Indicators of Compromise (IOCs). *This situation highlights the criticality of operating a vulnerability management program.*

References

- https://www.cisa.gov/emergency-directive-22-03
- https://nvd.nist.gov/vuln/detail/CVE-2022-22954
- https://www.vmware.com/security/advisories/VMSA-2022-0011.html
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-22954