VMware Security Response Center (vSRC) Response to ‘ESXiArgs’ Ransomware Attacks

2023-02-24 - Arnis Morkāns - Comments (0) - General

VMware has not found evidence that suggests an unknown vulnerability (0-day) is being used to propagate the ransomware used in these recent attacks. Most reports state that End of General Support (EOGS) and/or out-of-date products are being targeted with known vulnerabilities, which have been previously addressed and disclosed in VMware Security Advisories (VMSAs). You can sign up for email and RSS alerts when an advisory is published or significantly modified on our main VMSA page.

With this in mind, we are advising customers to upgrade to the latest available supported releases of vSphere components to address all currently disclosed vulnerabilities. In addition, VMware has recommended disabling the OpenSLP service in ESXi. ESXi 7.0 U2c and newer, and ESXi 8.0 GA and newer, ship with the service disabled by default.

VMware also has general ransomware resources available at our Ransomware Resource Center, as well as a frequently asked questions list about ESXiArgs, and information about security and lifecycle features in vSphere.

VMware Security Response Center (vSRC) Response to 'ESXiArgs' Ransomware Attacks - VMware Security Blog - VMware