Mphasis
The Next Applied

VMWare ESXi Ransomware Advisory

Severity: High

Date: 09th Feb 2023

Description

ESXi servers worldwide with a new ransomware strain dubbed “ESXiArgs.” The campaign appears to be leveraging CVE-2021-21974, a nearly two-year-old heap overflow vulnerability in the OpenSLP service ESXi runs. OpenSLP as used in ESXi has a heap-overflow vulnerability. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of 8.8.

Affected Versions

Who is running Unpatched (CVE-2021-21974) ESXi machines, exposed to the internet with port 427. CVE-2021-21974 affects the following systems:

- ESXi versions 7.x prior to ESXi70U1c-17325551
- ESXi versions 6.7.x prior to ESXi670-202102401-SG
- ESXi versions 6.5.x prior to ESXi650-202102101-SG

Recommendation

- Patch to latest version
- Deactivate the OpenSLP service on the server or to restrict access to only trusted IP addresses
- Check if the file “vmtools.py” is present in the “/store/packages/” location. If it is found, it is recommended to delete the file immediately.

Indicators of compromise

SHA 256 Hash Values

- 10c3b6b03a9bf105d264a8e7f30dcab0a6c59a414529b0af0a6bd9f1d2984459
- 11b1b2375d9d840912cfd1f0d0d04d93ed0cddb0ae4ddb550a5b62cd044d6b66
- 4fa565cc2ebfe97b996786facdb454e4328a28792e27e80e8b46fe24b44781af
- Dc90560d7198bf824b65ba2cfbe403d84d38113f41a1aa2f37f8d827fd9e0ceb
- 0cd7b6ea8857ce827180342a1c955e79c3336a6cf2000244e5cfd4279c5fc1b6
- 3a08e3bfec2db5dbece359ac9662e65361a8625a0122e68b56cd5ef3aedf8ce1
- 6a0449a0b92dc1b17da219492487de824e86a25284f21e6e3af056fe3f4c4ec0
- 2e52494e776be6433c89d5853f02b536f7da56e94bbe86ae4cc782f85bed2c4b
- 1cbbf108f44c8f4babde546d26425ca5340dccf878d306b90eb0fbec2f83ab51
- ea1872b2835128e3cb49a0bc27e4727ca33c4e6eba1e80422db19b505f965bc4
- 8f3db63f70fad912a3d5994e80ad9a6d1db6c38d119b38bc04890dfba4c4a2b2
- 0d6c3de5aebbbe85939d7588150edf7b7bdc712fceb6a83d79e65b6f79bfc2ef
- 984ce69083f2865ce90b48569291982e786980aeef83345953276adfcbbeece8
- 9cc3c217e3790f3247a0c0d3d18d6917701571a8526159e942d0fffb848acffb
- c93e6237abf041bc2530ccb510dd016ef1cc6847d43bf023351dce2a96fdc33b
- da3bb9669fb983ad8d2ffc01aab9d56198bd9cedf2cc4387f19f4604a070a9b5
- cb408d45762a628872fa782109e8fcfc3a5bf456074b007de21e9331bb3c5849
- 7594bf1d87d35b489545e283ef1785bb2e04637cc1ff1aca9b666dde70528e2b
- 039e1765de1cdec65ad5e49266ab794f8e5642adb0bdeb78d8c0b77e8b34ae09
- f3a1576837ed56bcf79ff486aadf36e78d624853e9409ec1823a6f46fd0143ea
- 95776f31cbcac08eb3f3e9235d07513a6d7a6bf9f1b7f3d400b2cf0afdb088a7
- 4bb2f87100fca40bfbb102e48ef43e65
- 80cfb7904e934182d512daa4fe0abbfb
- 9df15f471083698b818575c381e49c914dee69de

To Deactivate the OpenSLP Port 427

https://kb.vmware.com/s/article/76372

Recovery Script

https://www.cisa.gov/uscert/ncas/current-activity/2023/02/07/cisa-releases-esxiargs-ransomware-recovery-script

Reference Links

https://www.vmware.com/security/advisories/VMSA-2021-0002.html

https://blog.cyble.com/2023/02/06/massive-ransomware-attack-targets-vmware-esxi-servers/