U UNISPHERE SOLUTIONS

✉ info@unisphere.co.nz
🌐 www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00063

VMWARE ISSUES UPDATE FOR PREVIOUS FIX

DATE ISSUED: 10th November 2020

IMPACT	LOW	MEDIUM	▼ HIGH
EASE OF EXPLOIT	HARD ▼	MEDIUM	EASY

OVERVIEW

A previously issued security patch for Oracle's VMWare CVE-2020-3992 fix has been deemed incomplete and an update has been release to fix a Remote Code Execution (RCE) in the ESXi hypervisor.

BREAKDOWN

The initial patch released on 20//10/2020 did not fully address the vulnerability in the OpenSLP Use After Free (UAF) feature of VMWare ESXi which allows the discovery of network services available on a network. This particular flaw relates to dynamic memory being incorrectly utilised during the popular hypervisor's operation where the pointers in memory are not cleared once the location is freed. A malicious actor with access to port 427 on ESXi may be able to remotely execute arbitrary code. This vulnerability affects versions 3.x, 4.x, 6.5, 6.7 and 7.0. Patches are available for version 6.5, 6.7 and 7 while the others remain pending.

REMEDIATION STEPS

- Ensure all devices using VMWare EXSi from the list above are running the latest version where possible by updating using advice from the VMWare advisory below
- Continue to monitor for new security patches and updates issued by Oracle/VMWare

REFERENCES & RESOURCES

Threatpost	https://threatpost.com/vmware-updated-fix-critical-esxi-flaw/160944/
VMWare Advisory	https://www.vmware.com/security/advisories/VMSA-2020-0023.html