CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-051

VMware ESXi OpenSLP – Remote Code Execution Vulnerability

October 21, 2020 — v1.0

TLP:WHITE

Summary

On the 20th of October 2020, VMware released a security advisory for a vulnerability affecting ESXi OpenSLP, identified as CVE-2020-3992 [1]. OpenSLP as used in VMware ESXi has a use-after-free issue. VMware has evaluated the severity of this issue to be in the **critical severity** range with a maximum CVSSv3 base score of 9.8 out of 10.

Technical Details

A malicious actor residing in the management network who has access to port 427 on an ESXi machine may be able to trigger a use-after-free in the OpenSLP service resulting in remote code execution. The specific flaw exists within the processing of SLP messages. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the SLP daemon. Authentication is not required to exploit this vulnerability.

A full description of the vulnerability is available on Zero Day Initiative analysis [2].

Products Affected

- ESXi 7.0 before ESXi_7.0.1-0.0.16850804
- ESXi 6.7 before ESXi670-202010401-SG
- ESXi 6.5 before ESXi650-202010401-SG

Recommendations

To remediate CVE-2020-3992 apply the patches listed in the *Fixed Version* column of the *Response Matrix* found in the VMware advisory [1]. It is strongly advised to apply the security update from VMware to fix this vulnerability as soon as possible.

Workarounds

VMware has identified an workarounds for this vulnerability, the KB76372 [3].

References

[1] https://www.vmware.com/security/advisories/VMSA-2020-0023.html

[2] https://www.zerodayinitiative.com/advisories/ZDI-20-1269/

[3] https://kb.vmware.com/s/article/76372