Advisory Alert

Alert Number: AAA20201219 **Date:** December 19, 2020

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SolarWinds	**Critical**	Remote Code Execution
VMware	**Low**	Denial of Service

Description

Affected Product	SolarWinds
Severity	**Critical**
Affected Vulnerability	Remote Code Execution
Description	This Vulnerability is identified as SUNBURST backdoor, and it can communicate to third-party servers using HTTP. Using this vulnerability, already an attack has been made using SolarWinds Orion IT monitoring and management software. The backdoor is loaded by the actual SolarWinds executable before the legitimate code, specifically a component called SolarWinds.Orion.Core.BusinessLayer.dll.
Affected Products	Orion Platform v2020.2 HF 1 Orion Platform v2019.4 HF 5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.solarwinds.com/securityadvisory

Affected Product	VMware
Severity	**Low**
Affected Vulnerability	Denial of Service (CVE-2020-3999)
Description	VMware has released security patch updates addressing vulnerability that exist in their products. VMware ESXi, Workstation and Fusion contain a denial of service vulnerability due to improper input validation in GuestInfo. A malicious actor with normal user privilege access to a virtual machine can crash the virtual machine's vmx process leading to a denial of service condition.
Affected Products	VMware ESXi VMware Workstation VMware Fusion
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2020-0029.html

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.