Windows Installer Zero-Day

Malware actively exploiting new Windows Installer Zero-Day

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-41379
CVEs: CVE-2021-41379

A new Windows Installer Zero-Day is actively being exploited by malware.

Background

Microsoft announced a vulnerability on Windows Installer as part of their Patch Tuesday. A security researcher discovered that the patch was not enough and have posted a proof of concept.

Announced

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-41379

https://www.bleepingcomputer.com/news/security/malware-now-trying-to-exploit-new-windows-installer-zero-day/

https://threatpost.com/attackers-target-windows-installer-bug/176558/

https://thehackernews.com/2021/11/warning-hackers-exploiting-new-windows.html

Latest Developments

On November 9, 2021, Microsoft announced a privilege escalation vulnerability on Windows Installer. A couple weeks later, security researcher Abdelhamid Naceri posted a proof of concept further exploiting the already-patched Windows Installer. Based on FortiGuard statistics from the last few days, Malware using this vulnerability is active in the wild.

Fortinet Products Summary

	Services	Version	Other Info
FortiGate	AV	*89.07141*	
FortiClient	AV	*89.07141*	
FortiEDR	AV (Pre-Filter)	*89.07141*	
FortiSandbox	AV (Pre-Filter)	*89.07141*	
FortiAI	AV (Pre-Filter)	*89.07141*	
FortiMail	AV	*89.07141*	
FortiCASB	AV	*89.07141*	
FortiCWP	AV	*89.07141*	
FortiADC	AV	*89.07141*	
FortiProxy	AV	*89.07141*	
FortiAnalyzer	Event Handlers & Reports	*6.4*	
FortiSIEM	Rules & Reports	*TBC*	

Cyber Kill Chain

Reconnaissance

Weaponization

Delivery

FortiGate
AV
Version Info: 89.07141
Link: W32/CVE_2021_41379.A!exploit W32/CVE_2021_41379.A!tr

FortiClient
AV
Version Info: 89.07141
Link: W32/CVE_2021_41379.A!exploit W32/CVE_2021_41379.A!tr

FortiEDR
AV (Pre-Filter)
Version Info: 89.07141
Link: W32/CVE_2021_41379.A!exploit W32/CVE_2021_41379.A!tr

FortiSandbox
AV (Pre-Filter)
Version Info: 89.07141
Link: W32/CVE_2021_41379.A!exploit W32/CVE_2021_41379.A!tr

FortiAI
AV (Pre-Filter)
Version Info: 89.07141
Link: W32/CVE_2021_41379.A!exploit W32/CVE_2021_41379.A!tr

FortiMail
AV
Version Info: 89.07141
Link: W32/CVE_2021_41379.A!exploit W32/CVE_2021_41379.A!tr

FortiCASB
AV
Version Info: 89.07141
Link: W32/CVE_2021_41379.A!exploit W32/CVE_2021_41379.A!tr

FortiCWP
AV
Version Info: 89.07141
Link: W32/CVE_2021_41379.A!exploit W32/CVE_2021_41379.A!tr

FortiADC
AV
Version Info: 89.07141
Link: W32/CVE_2021_41379.A!exploit W32/CVE_2021_41379.A!tr

FortiProxy
AV
Version Info: 89.07141
Link: W32/CVE_2021_41379.A!exploit W32/CVE_2021_41379.A!tr

Exploitation

Installation

C2

Action

Endpoint

Incident Response (Security Operations)

To help customers identify and protect vulnerable, FortiAnalyzer, FortiSIEM and FortiSOAR updates are available to raise alerts and escalate to incident response:

Analyzer / SIEM / SOAR Threat Hunting & Playbooks

FortiAnalyzer
Event Handlers & Reports
Version Info: 6.4
Link:

FortiSIEM
Rules & Reports
Version Info: TBC
Link: