Microsoft PrintNightmare

Public 0-day exploit allows domain takeover

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

CVEs: CVE-2021-34527

A remote code execution vulnerability exists in Windows OS when the Windows Print Spooler service improperly performs privileged file operations. An attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Microsoft is encouraging customers to either "Disable the Print Spooler service" or "Disable inbound remote printing through Group Policy". https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Background

On June 30 it was disclosed that the technical details and a proof-of-concept (PoC) exploit have been accidentally leaked for a currently unpatched vulnerability in Windows that allows remote code execution. Despite the need for authentication, the severity of the issue is critical as threat actors can use it to take over a Windows domain server to easily deploy malware across a company's network. The issue affects Windows Print Spooler and the researchers named it PrintNightmare.

https://www.bleepingcomputer.com/news/security/public-windows-printnightmare-0-day-exploit-allows-domain-takeover/

Announced

June 30: Initial details emerge -

https://www.bleepingcomputer.com/news/security/public-windows-printnightmare-0-day-exploit-allows-domain-takeover/

Latest Developments

July 7 - Full patch / fix released -

https://www.bleepingcomputer.com/news/security/microsoft-printnightmare-now-patched-on-all-windows-versions/

July 6 - Microsoft released a security patch (found later to be a partial fix) -

https://us-cert.cisa.gov/ncas/current-activity/2021/07/06/microsoft-releases-out-band-security-updates-printnightmare

July 2 - Microsoft is investigating the vulnerability and assigned a CVE to the vulnerability -

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

Fortinet Products Summary

	Services	Version	Other Info
FortiGate	**IPS**	*6.0+*	FortiGuard IPS blocks the Exploit
FortiClient	**Vulnerability**	*6.2+*	Detects Vulnerable Endpoints and triggers Auto-Patching
FortiAnalyzer	**Event Handlers & Reports**	*6.2+*	Detects vulnerable endpoints and intrusion attempts against the network, covering FortiGate and FortiClient
FortiSIEM	**Rules & Reports**	*6.2+*	Detects vulnerable endpoints and intrusion attempts against the network, covering FortiGate, FortiClient and 3rd party products

Cyber Kill Chain

Reconnaissance

Weaponization

Delivery

FortiClient
Vulnerability
Version Info: 1.251
Link: https://www.fortiguard.com/updates/epvuln?version=1.251

Exploitation

FortiGate
IPS
Version Info: 18.109
Link: https://www.fortiguard.com/updates/ips?version=18.109

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: 6.2+
Link: https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FD52678

FortiSIEM
Rules & Reports
Version Info: 6.2+
Link: https://kb.fortinet.com/kb/microsites/microsite.do?cmd=displayKC&docType=kc&externalId=FD52679