Public 0-day utilizing domain takeover

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 software; view, change, or delete data; or create new accounts with full user rights.

Microsoft PrintNightmare

CVEs:

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

Public 0-day exploit allows domain takeover

July 2, 2021 - Microsoft is investigating the vulnerability and assigned a CVE to the vulnerability - CVE-2021-34527

July 6, 2021 - Microsoft released a security patch (found later to be a partial fix) - https://www.bleepingcomputer.com/news/security/microsoft-printnightmare-now-patched-on-all-windows-vista-and-older/

July 7, 2021- Full patch / fix released - https://www.cisa.gov/uscert/ncas/alerts/aa22-074a


March 15, 2022 - CISA reported that Russian state sponsored hackers have exploited this vulnerability in Windows Print Spooler and the researchers named it PrintNightmare.

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.


FortiSOAR updates are available to raise alerts and escalate to incident response:

FortiSOAR updates are available to raise alerts and escalate to incident response: FortiAnalyzer, FortiSIEM and FortiProxy.

To help customers identify and protect vulnerable endpoints, FortiAnalyzer, FortiSIEM and FortiProxy can detect Windows PrintNightmare vulnerability.

Fortinet’s cyber Kill-Chain

Insight Response (Security Operations)