

## Microsoft PrintNightmare Vulnerability

### 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".

**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.

**Announced** June 30: Initial details emerge  
<https://www.bleepingcomputer.com/news/security/public-windows-printnightmare-0-day-exploit-allows-domain-takeover/>

**Latest Developments** March 15, 2022 - CISA reported that Russian state sponsored hackers have exploited this vulnerability in combination with default Multi-Factor Authentication protocols to gain access to cloud and email accounts for document exfiltration. - <https://www.cisa.gov/uscert/ncas/alerts/aa22-074a>  
 July 7, 2021- Full patch / fix released - <https://www.bleepingcomputer.com/news/security/microsoft-printnightmare-now-patched-on-all-windows-versions/>  
 July 6, 2021 - 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, 2021 - Microsoft is investigating the vulnerability and assigned a CVE to the vulnerability - <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527>


## PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

### Reconnaissance

#### Decoy VM

Detect activities on exploitation of PrintSpooler vulnerability.



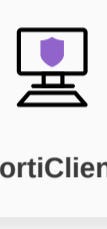
FortiDeceptor  
v3.0+

### Weaponization

### Delivery

#### Vulnerability

Detects Vulnerable Endpoints and triggers Auto-Patching








FortiClient  
DB 1.251

### Exploitation

#### IPS

Detect activities on exploitation of PrintSpooler vulnerability

FortiGate DB 18.109 FortiSASE DB 18.109 FortiNDR DB 18.109 FortiADC DB 18.109 FortiProxy DB 18.109

### Installation


### C2

### Action

## DETECT



Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

### Outbreak Detection



FortiAnalyzer  
DB 1.00027

### Threat Hunting


FortiAnalyzer DB 6.2+ FortiSIEM DB 6.2+

## RESPOND

Develop containment techniques to mitigate impacts of security events:

### Automated Response


Services that can automatically respond to this outbreak.



FortiXDR

### Assisted Response Services

Experts to assist you with analysis, containment and response activities.





Incident Response

## RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

### NOC/SOC Training


Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

NSE Training Response Readiness

### End-User Training

Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.





Security Awareness & Training

## IDENTIFY

Identify processes and assets that need protection:

### Attack Surface Hardening


Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Security Rating CNP

### Vulnerability Management

Reduce the attack surface on software vulnerabilities via systematic and automated patching.



FortiClient

## Additional Resources

- Bleeping Computer** <https://www.bleepingcomputer.com/news/security/microsoft-printnightmare-now-patched-on-all-windows-versions/>
- Threat Post** <https://threatpost.com/microsoft-unpatched-printnightmare-zero-day/168613/>
- CISA Alert** <https://www.cisa.gov/uscert/ncas/alerts/aa22-074a>

Learn more about [FortiGuard Outbreak Alerts](#)