# PrintNightmare vulnerability weaponized by Magniber ransomware gang

therecord.media/printnightmare-vulnerability-weaponized-by-magniber-ransomware-gang/

August 12, 2021

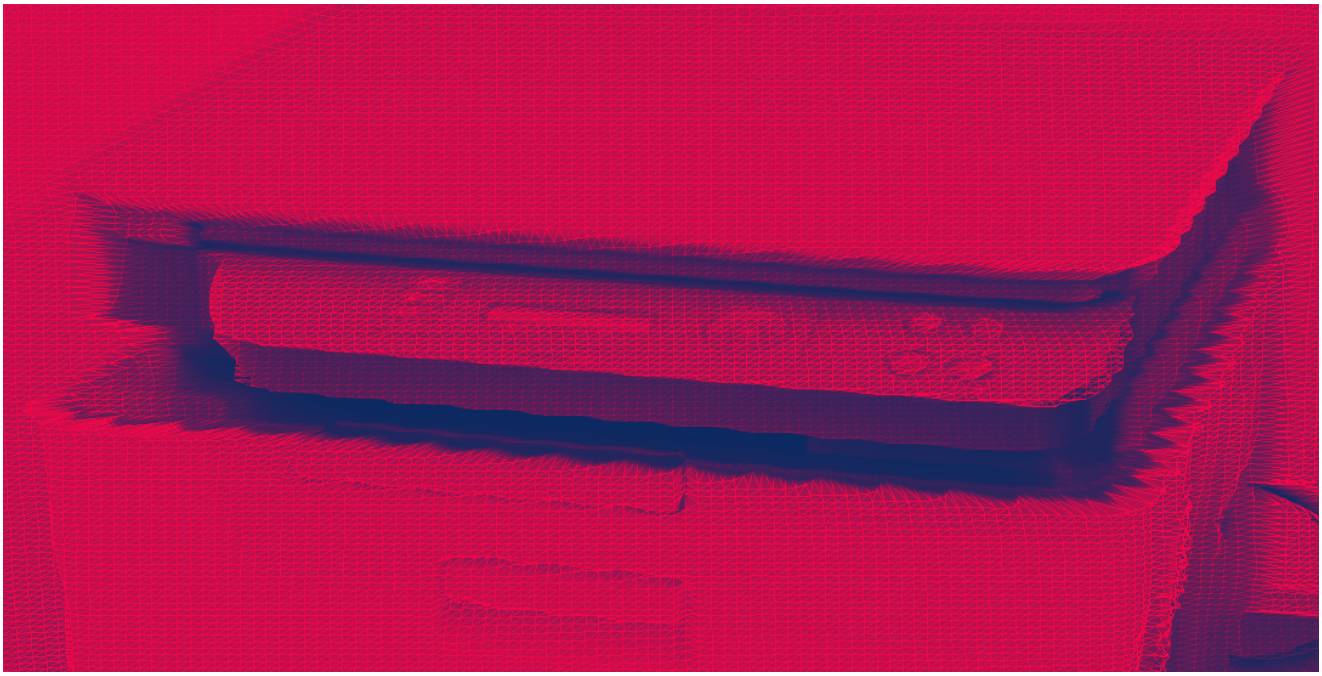

Image: Mahrous Houses

The operators of the Magniber ransomware have weaponized the infamous PrintNightmare vulnerability and are now attempting to breach Windows systems in South Korea.

In a report published today by security firm CrowdStrike, the company said the attacks have been taking place since at least July 13.

### Which PrintNightmare is this?

While several different vulnerabilities in the Windows Print Spooler service are collectively referred to as PrintNightmare, CrowdStrike said the attackers weaponized CVE-2021-34527.

This is one of the two original PrintNightmare bugs that started this whole series of vulnerabilities, which is now getting close to around 10 different issues.

Initially tracked and (believed to have been) patched in early June as CVE-2021-1675, researchers published proof of concept code to exploit this bug in late June.

The proof-of-concept code was pulled down within hours after researchers realized it was exploiting a different issue, a much worse one, but by that time, the cat was out of the bag.

- CVE-2021-1675 – elevation of privilege bug in Print Spooler server

- CVE-2021-34527- remote code execution in Print Spooler server

Microsoft assigned CVE-2021-34527 to this new bug and patched it two weeks later, on July 6.

Since then, several other variations of these two initial PrintNightmare bugs have been discovered in the Print Spooler service, including one discovered a day after this month's Patch Tuesday and still unpatched, all still collectively called PrintNightmare.

### Attacks limited to South Korea, for now

While several security experts anticipated that PrintNightmare would be exploited in the wild, especially the RCE variant, for now, the attacks have been limited to South Korea.

First spotted in late 2017, the Magniber ransomware has exclusively been active only in South Korea.

While CrowdStrike has not published an attack chain for the recent Magniber-PrintNightmare attacks, it is worth mentioning that the Magniber group has been using the Magnitude exploit kit to distribute its payloads since at least 2018, an exploit kit which it still uses today, according to Avast.

An exploit kit is a web-based app designed to infect users by exploiting browser vulnerabilities.

Tags

- Crowdstrike
- Magniber
- Magnitude EK
- Print Spooler
- PrintNightmare
- Ransomware
- South Korea
- vulnerability
- Windows

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.