The 'PrintNightmare' threat and Lasernet service

2021-07-05 - Alex Clemons - Comments (0) - Lasernet News

There have been some recent published recommendations from Microsoft regarding the 'PrintNightmare' threat. This involves a Windows Print Spooler remote code execution vulnerability.

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

Multiple components of Lasernet (beyond just the physical printing of documents) rely on the Print Spooler Service to be able to function successfully and so deactivating the Spooler Service means that the Lasernet server becomes unusable. If users deactivate the LPD service, the Lasernet server will not receive any jobs (from AS400 for example).

In summary, the Lasernet service depends on the Print Spooler Service to function, so we recommend that it is not deactivated on the Lasernet server.

LATEST

Microsoft have recently started rolling out Windows Updates to all major OS versions (exact KB numbers can be found in the above article).

Following these releases, our Product team has tested Lasernet 9 and 10 with the latest Windows Updates and have found:

- No known memory or handle leaks
- Printer profiles validated
- JobInfos set Docname, username and copies for print queue validated
- Installing printer drivers are validated

Our testing has not identified any clear impact to Lasernet or the Lasernet Service by installing these Windows Updates.

However, testing can never be seen as fully comprehensive; we test with a variety of different situations but can never test with all situations. So before upgrading production systems with the latest Windows Updates, it is advised to test all configurations on a

Test/Development server to verify each bespoke configuration to ensure no data or print driver-specific issues can occur.

Related Content

- PrintNightmare Update Issue – Windows Update on Server and Client Out of Date