

The PrintNightmare threat and Lاسernet service

Flemming Larsen - 2022-12-21 - Comments (0) - Lاسernet General Information

Lاسernet

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 Lاسernet (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 Lاسernet server becomes unusable. If users deactivate the LPD service, the Lاسernet server will not receive any jobs (from AS400 for example).

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

Note

This exploit has been patched on 21/09/2021 with patch "KB5005625", any machine updated since then should not be affected by this vulnerability.