

# High Risk Vulnerability in Lexmark Printer Sharing Service

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2006-02/msg00107.html>

---

- *From:* "NGSSoftware Insight Security Research" <[nisr@xxxxxxxxxxxxxxxx](mailto:nisr@xxxxxxxxxxxxxxxx)>
  - *Date:* Tue, 7 Feb 2006 14:12:53 -0000
- 

Peter Winter-Smith of NGSSoftware has discovered a high risk vulnerability in the Lexmark Printer Sharing service which could allow a remote, unauthenticated attacker to execute arbitrary code on a Lexmark printer user's computer system with Local System privileges.

There is no known official patch or workaround for this issue, as Lexmark have proven unresponsive throughout the investigation and have failed to provide us with a response to our queries on many occasions.

Communications between NGS and Lexmark to date are summed up in the following time-line:

[28/09/2005] Initial email to support@xxxxxxxxxxx  
[28/09/2005] Automated reply from support@xxxxxxxxxxx  
[29/09/2005] Re-sent email to csupportuk@xxxxxxxxxxxxxxxx .. No response  
[03/10/2005] Mass mail to secure@xxxxxxxxxxx, security@xxxxxxxxxxx, security-alert@xxxxxxxxxxx, info@xxxxxxxxxxx .. No response  
[04/10/2005] First response from Lexmark's 'Task ID IE THIRD LEVEL ESCALATIONS' thanking NGS for the email dated the 28th Sept. asking for further details.  
[04/10/2005] Details of the vulnerability provided to Lexmark .. No response  
[11/10/2005] Follow-up email to Lexmark .. No response  
[18/10/2005] Follow-up email to Lexmark .. No response  
[24/10/2005] Follow-up email to Lexmark .. No response  
[08/11/2005] Follow-up email to Lexmark .. No response  
[30/12/2005] Follow-up email to Lexmark .. No response  
[07/01/2006] Informing Lexmark of this advisory .. No response

From our tests it seems that the following workaround will prevent the

vulnerability from being present by removing the vulnerable service so that it cannot start. This should not prevent the printer from working in normal operations, however if a user is depending on the Lexmark Printer Sharing services for network printing this workaround may impact that level of functionality.

NGS do not take any responsibility for the following information being

## High Risk Vulnerability in Lexmark Printer Sharing Service

correct or for any of the results which may occur as a result of taking the following actions.

Workaround:

1. Launch the Services console by taking the following actions:
  - Click the 'Start' menu.
  - Select 'Run'.
  - In the 'Run' command text area type 'services.msc' and click 'Ok'.
2. Find and right click the 'LexBce Server' entry. From the right click menu select the 'Stop' item. Confirm that you wish to stop the service and all dependencies.
3. Open the '%systemroot%\system32' folder by taking the following actions:
  - Click the 'Start' menu.
  - Select 'Run'.
  - In the 'Run' command text area type '%systemroot%\system32' and click 'Ok'.
4. Locate the file named 'LexPPS.EXE'. Right click this file and select 'Rename'. Enter a new name for the file, I recommend 'LexPPS.EXE.vuln'.
5. In the Services console, locate and right click the 'LexBce Server' and select 'Start'.
6. In the Services console, locate and right click the 'Print Spooler' and select 'Start'.

This disclosure was made in accordance with the NGS responsible disclosure policy which can be viewed online at:

<http://www.ngssoftware.com/disclosure.pdf>

NGSSoftware will withhold technical details of this flaw for at least one month. Full technical details will be published on or after the 7th March 2006.

NGSSoftware Insight Security Research

<http://www.ngssoftware.com>

<http://www.databasesecurity.com/>

<http://www.nextgenss.com/>

+44(0)208 401 0070