Dear FlexNet Publisher Customer,

While there are no reported exploits, we want to inform you as early as possible that four vulnerabilities have recently been discovered in FlexNet Publisher. Below you will find all the details you need. A fix will be available with the next release, FlexNet Publisher 2018 R4, planned for December 20, 2018.

Please be aware that network access to the FlexNet Publisher License Server would be necessary to perform any attack. Protecting the license server from unauthorized access is essential to minimize the opportunities for any of the vulnerabilities to be exploited.

The vulnerabilities have been discovered by Kaspersky Lab ICS-CERT. It is likely that Kaspersky will disclose related information at their Off Zone conference in Moscow on November 15-16, 2018.

Which versions are affected?

All versions of FlexNet Publisher (2018 R3 and prior) are likely affected.

What is the vulnerability?

Three of the reported vulnerabilities can be exploited to cause a DoS (Denial of Service). One can be exploited to potentially allow execution of arbitrary code, although we are not aware that any exploit has been developed to prove this.

The most severe vulnerability has been assigned the CVSSv3 score of 8.8 base score and an 8.3 temporal score. The Secunia Research Advisory criticality is “Moderately Critical” (3 out of 5). More information on terminology is available here.

When will a patch be available and what actions will customers have to take?

The vulnerabilities will be patched in the next release, FlexNet Publisher 2018 R4 (11.16.2), which is planned for December 20, 2018. We recommend all customers using affected versions of FlexNet Publisher to upgrade to version 2018 R4 when available. We will notify you as soon as the new release is available.

We advise all FlexNet Publisher customers update lmgrd as soon as FlexNet Publisher 11.16.2 is available, and the vendor daemon as soon as possible after that.

Please note that lmadmin is not affected.

Customers are also strongly advised to follow best practice in protecting the license server from unauthorized access.

What will Kaspersky disclose?

The vulnerabilities mentioned above have been reported by Kaspersky. They will likely disclose high-level information about the vulnerabilities but will not provide instructions on how to exploit it. Any disclosure is likely to happen at their Off Zone conference in Moscow.

Please note that Kaspersky might mention five vulnerabilities (not four). Two of the vulnerabilities they reported have the same root cause and are therefore defined as one. You might also see a statement that two vulnerabilities might allow remote code execution (not one). After in-depth research we consider that an incorrect

conclusion.

They have also raised questions related to the lmdown command in FlexNet Publisher and the chance that this might be used by a remote attacker. Their argument is that lmdown can be executed remotely to bring the server down. However, it is best practice to start lmgrd with the options -2 -p local so that local administrator access is required to run lmdown.

Who do I contact if I have more questions?

If you have any questions, please contact Technical Support.

We apologize for the inconvenience. We strive to deliver a high-quality product and the best experience possible for you. We are doing our utmost to prevent situations like this and to mitigate vulnerabilities as fast as possible if they do occur.

We thank you for your continued support.

Your Flexera Team