Rootshell Discover a Denial of Service Flaw in NetLib Security's Encryptionizer Platform

Rootshell's Research and Development team have discovered a flaw in NetLib Security's flagship encryption platform, Encryptionizer, and its associated kernel drivers.

The team have discovered numerous flaws in a common component of the Encryptionizer implementation, which arise when an IOCTL request is sent by a local user/program to the kernel driver. The request can cause the driver to perform privileged operations on arbitrary HANDLE's, along with access to what is thought to be testing functionality.

The root cause of the issues is that the kernel driver is written in such a way as to trust the input from the user land program. Therefore, access to the kernel driver is 'obfuscated' to prevent simplistic access to the driver interface through the file system minifilter API interface.

The team have developed a simple proof of concept (POC) of the issue, which will crash any affected system.

The POC exploits an arbitrary call to the KeBugCheckEx function from the affected kernel driver, resulting in a Denial of Service (DoS) through a BSOD (Blue Screen of Death) of the kernel.

In line with our Bug Release Terms, we informed NetLib Security of these issues and gave 90 days of notice before disclosing any information. Limited information relating to these issues will be disclosed. However, more detailed information relating to the Denial of Service (DoS) issues is provided, as the severity of such releases is limited.

September 22nd, 2021

Share This Story, Choose Your Platform!

Related Posts

Rootshell’s Open-Source CVSS Calculator is a Hit

Prism Platform New Dashboa Is More Interacti

Services

≡

Prism

≡

Resources

≡

Company

≡

Rootshell Security

info@rootshellsecurity.net

UK +44 1256 596523

USA +1 332 225 1894

Subscribe for Updates *

✉

Your data will be processed in accordance with our Privacy Policy

Subscribe