Security Advisory 2022-042

Critical Vulnerability in Windows NFS

June 15, 2022 — v1.0

TLP:WHITE

History:

- *15/06/2022 — v1.0 – Initial publication*

Summary

On the 14th of June 2022, Microsoft – as part of the June Patch Tuesday release – has issued several (55) security fixes for various vulnerabilities. Among others, the update fixes the **critical vulnerability** `CVE-2022-30136` which is a RCE vulnerability in the network file system (NFS). The vulnerability can be exploited by an **unauthenticated attacker** using a specially crafted call to a NFS service [1]. The vulnerability is not exploitable in NFSV2.0 or NFSV3.0 [2].

There is no evidence that this vulnerability is exploited in the wild. However, it is recommended to patch as soon as possible.

Technical Details

The vulnerability tracked as `CVE-2022-30136` (CVSS score: 9.8) affects Windows assets running NFS. This vulnerability is not exploitable in NFSV2.0 or NFSV3.0 [2]. Microsoft has not provided more technical details about this vulnerability at this time.

Affected Products

This vulnerability affects the following Windows products with NFS enabled (also Server Core installation):

- Windows Server 2012 R2;
- Windows Server 2012;
- Windows Server 2016;
- Windows Server 2019.

Recommendations

CERT-EU recommends to apply the patches provided by Microsoft as soon as possible.

Mitigations

The advisory notes that NFS versions 2.0 and 3.0 are not affected and administrators can disable NFS version 4.1 to mitigate this flaw [2].

References

[1] https://www.tenable.com/blog/microsofts-june-2022-patch-tuesday-addresses-55-cves-cve-2022-30190

[2] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30136

[3] https://media.cert.europa.eu/static/SecurityAdvisories/2022/CERT-EU-SA2022-039.pdf