

[Home](#)

Advisories

Currently published 96 advisories.

[Vulnerability Disclosure Policy](#)

(CVE-2021-4206) QEMU QXL Integer overflow leads to Heap Overflow

CVE: CVE-2021-4206 Tested Versions: QEMU < v6.0.0 Product URL(s): <https://www.qemu.org/> Description of the vulnerability Technical Details QXL, the QEMU QXL video accelerator, is a para-virtualized framebuffer...

March 28, 2022 · 3 min · Billy Jheng Bing Jhong (@st424204)

(CVE-2021-4207) QEMU QXL Integer overflow leads to Heap Overflow

CVE: CVE-2021-4207 Tested Versions: QEMU < v6.0.0 Product URL(s): <https://www.qemu.org/> Description of the vulnerability Technical Details QXL, the QEMU QXL video accelerator, is a para-virtualized framebuffer...

March 28, 2022 · 3 min · Billy Jheng Bing Jhong (@st424204)

(CVE-2022-0168) Linux Kernel smb2_ioctl_query_info NULL Pointer Dereference

CVE: CVE-2022-0168 Tested Versions: Linux kernels 5.4–5.12, 5.13-rc+HEAD Description of the vulnerability Common Internet File System (CIFS) is a network filesystem protocol used for providing shared access to...

March 28, 2022 · 4 min · Billy Jheng Bing Jhong (@st424204)

(CVE-2022-0216) QEMU LSI SCSI Use After Free

CVE: CVE-2022-0216 Tested Versions: QEMU < v6.0.0 Product URL(s): <https://www.qemu.org/> Description of the vulnerability Technical Details The vulnerability resides in the hw/scsi/lscsi53c895a.c specifically in...

March 28, 2022 · 7 min · Muhammad Alifa Ramdhan (@n0psledbyte)

(CVE-2022-28730) Apache JSPWiki v2.11.1 - Reflected XSS in AjaxPreview.jsp

CVE: CVE-2022-28730 Tested Versions: Latest release v2.11.2 CVSSv3.1 Base Score: 5.4 (Medium) CVSSv3.1 String: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N Product URL(s): <https://github.com/apache/jspwiki/>...

March 14, 2022 · 1 min · Poh Jia Hao

(CVE-2022-26718) macOS smbfs Out-of-Bounds Read due to parse nic info

CVE: CVE-2022-26718 Tested Versions: macOS 11.x.x <= 11.6.4 macOS 12.x.x <= 12.2.1 Product URL(s): <https://www.apple.com/> Description of the vulnerability smbfs stands for Samba file system of macOS,...

March 4, 2022 · 4 min · Peter Nguyễn Vũ Hoàng

(CVE-2021-30844) macOS smbfs Out-of-Bounds Read

CVE: CVE-2021-30844 Tested Versions: macOS BigSur 11.0 - 11.2.3 Product URL(s): <https://apple.com> Description of the vulnerability smbfs is a next driver which handles SMB connection between the user and...

September 13, 2021 · 3 min · Peter Nguyễn Vũ Hoàng

[Next »](#)