Overall Rating - High

BRITISH COLUMBIA

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware of multiple vulnerabilities recently disclosed for the Linux kernel

Technical Details

- A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the processing of SMB2_SESSION_SETUP and SMB2_LOGOFF commands. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to execute code in the context of the kernel. CVE-2023-32257
- A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the processing of SMB2_LOGOFF and SMB2_CLOSE commands. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to execute code in the context of the kernel. CVE-2023-32258
- A possible unauthorized memory access flaw was found in the Linux kernel's cpu_entry_area mapping of X86 CPU data to memory, where a user may guess the location of exception stacks or other important data. Based on the previous CVE-2023-0597, the 'Randomize per-cpu entry area' feature was implemented in /arch/x86/mm/cpu_entry_area.c, which works through the init_cea_offsets() function when KASLR is enabled. However, despite this feature, there is still a risk of per-cpu entry area leaks. This issue could allow a local user to gain access to some important data with memory in an expected location and potentially escalate their privileges on the system. CVE-2023-3640

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- *Ensure mitigation is performed at your next change window.*

Please notify VRM with any questions or concerns you may have.

References

- CVE-2023-32257, CVE-2023-32258, CVE-2023-3640
- https://www.zerodayinitiative.com/advisories/ZDI-CAN-20596/
- https://bugzilla.redhat.com/show_bug.cgi?id=2219806
- https://access.redhat.com/security/cve/CVE-2023-32257
- https://bugzilla.redhat.com/show_bug.cgi?id=2219809

- https://access.redhat.com/security/cve/CVE-2023-32258
- https://www.zerodayinitiative.com/advisories/ZDI-CAN-20796/
- https://bugzilla.redhat.com/show_bug.cgi?id=2217523
- https://access.redhat.com/security/cve/CVE-2023-3640