

Overall Rating - High



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

Summary

The Vulnerability and Risk Management (VRM) Team is aware a vulnerability has been discovered in Node.js version 20, specifically within the experimental permission model.

Technical Details

This flaw relates to improper handling of Buffers in file system APIs causing a traversal path to bypass when verifying file permissions. This vulnerability affects all users using the experimental permission model in Node.js 20.

Please note that at the time this CVE was issued, the permission model is an experimental feature of Node.js.

This vulnerability is rated as a **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-2023-32004](#)
- <https://hackerone.com/reports/2038134>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/JQPELKG2LVTADSB7ME73AV4DXQK47PWK/>
- <https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/PBOZE2QZIBLFFTYWYN23FGKN6HULZ6HX/>