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 in .NET and Visual Studio

Technical Details

- **Denial of Service Vulnerability** - **CVE-2023-38180**
  See links below for more information.

- **Remote Code Execution Vulnerability - CVE-2023-35390**
  To exploit this vulnerability, an attacker would first have to log on to the system. An attacker could then run a specially crafted application that could exploit the vulnerability and take control of an affected system. Additionally, an attacker could convince a local user to open a malicious file. The attacker would have to convince the user to click a link, typically by way of an enticement in an email or instant message, and then convince them to open the specially crafted file.

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-2023-38180, CVE-2023-35390
- https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/CL2L4WE5QRT7WEXANYXSKSU43APC5N2V/
- https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/NWVZFKTLNMNKPZ755EMRYIA6GHFOWGKY/
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-38180
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35390