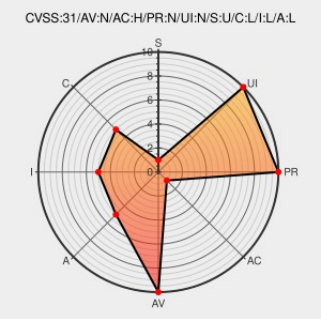
CVE-2022-39343

Published on: Not Yet Published

Last Modified on: 11/10/2022 12:32:00 AM UTC

CVE-2022-39343 - advisory for GHSA-8jqf-wjhq-4w9f

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Azure Rtos Filex from Microsoft contain the following vulnerability:

Azure RTOS FileX is a FAT-compatible file system that's fully integrated with Azure RTOS ThreadX. In versions before 6.2.0, the Fault Tolerant feature of Azure RTOS FileX includes integer under and overflows which may be exploited to achieve buffer overflow and modify memory contents. When a valid log file with correct ID and checksum is detected by the `_fx_fault_tolerant_enable` function an attempt to recover the previous failed write operation is taken by call of `_fx_fault_tolerant_apply_logs`. This function iterates through the log entries and performs required recovery operations. When properly crafted a log including entries of type `FX_FAULT_TOLERANT_DIR_LOG_TYPE` may be utilized to introduce unexpected behavior. This issue has been patched in version 6.2.0. A workaround to fix line 218 in fx_fault_tolerant_apply_logs.c is documented in the GHSA.

CVE-2022-39343 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **azure-rtos** - **filex** version **< 6.2.0**

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Fault Tolerant Overflow · Advisory · azure-rtos/filex · GitHub	github.com text/html	CONFIRM github.com/azure-rtos/filex/security/advisories/GHSA-8jqf-wjhq-4w9f
filex/fx_fault_tolerant_apply_logs.c at master ·	github.com	MISC github.com/azure-

azure-rtos/filex · GitHub

text/html

rtos/filex/blob/master/common/src/fx_fault_tolerant_apply_logs.c#L218

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Azure Rtos Filex	All	All	All	All

cpe:2.3:o:microsoft:azure_rtos_filex:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-39343 : Azure RTOS FileX is a FAT-compatible file system that’s fully integrated with Azure RTOS ThreadX.… twitter.com/i/web/status/1…	2022-11-08 07:38:52
/r/netcve	CVE-2022-39343	2022-11-08 08:38:41

← Previous ID

Next ID→