USBX Host CDC ECD integer underflow with buffer overflow

Moderate liydu published GHSA-chpp-5fv9-6368 on Oct 10

Package

USBX (Azure RTOS)

Affected versions	Patched versions
< 6.1.12	6.1.12

Description

Impact

Azure RTOS USBX implementation of host support for USB CDC ECM includes an integer underflow and a buffer overflow in the `_ux_host_class_cdc_ecm_mac_address_get` function which may be potentially exploited to achieve remote code execution or denial of service.

Setting mac address string descriptor length to a `0` or `1` allows an attacker to introduce an integer underflow followed (string_length) by a buffer overflow of the `cdc_ecm -> ux_host_class_cdc_ecm_node_id` array. This may allow one to redirect the code execution flow or introduce a denial of service.

Patches

We analyzed this bug and determined that we needed to fix it. This fix has been included in USBX release 6.1.12

Workarounds

Improve mac address string descriptor length validation to check for unexpectedly small values.

References

https://github.com/azure-rtos/usbx/blob/master/common/usbx_host_classes/src/ux_host_class_cdc_ecm_mac_address_get.c#L264

For more information

If you have any questions or comments about this advisory:

- Open an issue in azure-rtos/usbx
- Post question on Microsoft Q&A

Severity

Moderate

CVE ID

CVE-2022-36063

Weaknesses

No CWEs

Credits

 szymonh