



# NCSC-2024-0339

## Kwetsbaarheden verholpen in Microsoft Mariner

NCSC Advisory

Prioriteit: Normaal

Gepubliceerd op: 13-08-2024

**TLP:WHITE**

### Toegestane verspreiding van TLP:WHITE

(Traffic Light Protocol)

Deze handreiking bevat het label TLP:WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First ([www.first.org/tlp](http://www.first.org/tlp)).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op [info@ncsc.nl](mailto:info@ncsc.nl)

Feiten

Microsoft heeft kwetsbaarheden verholpen in Mariner (Azure Linux).

Duiding

De kwetsbaarheden betreffen oudere kwetsbaarheden in diverse subcomponenten van de distro, zoals Python, Emacs, Qemu, Django, Curl, wget etc. welke in de nieuwe versie zijn verholpen.

Oplossingen

Microsoft heeft updates beschikbaar gesteld waarmee de beschreven kwetsbaarheden worden verholpen. We raden u aan om deze updates te installeren. Meer informatie over de kwetsbaarheden, de installatie van de updates en eventuele work-arounds vindt u op:

<https://portal.msrc.microsoft.com/en-us/security-guidance>

Kwetsbaarheden

| CVE              | CVSS Score |
|------------------|------------|
| > CVE-2022-2601  |            |
| > CVE-2022-3775  |            |
| > CVE-2022-36648 |            |
| > CVE-2019-3833  |            |
| > CVE-2021-3929  |            |
| > CVE-2021-4158  |            |
| > CVE-2021-4206  |            |
| > CVE-2021-4207  |            |
| > CVE-2022-26353 |            |
| > CVE-2022-35414 |            |
| > CVE-2023-3354  |            |

|                  |
|------------------|
| > CVE-2022-3872  |
| > CVE-2022-4144  |
| > CVE-2023-45288 |
| > CVE-2023-29404 |
| > CVE-2023-29402 |
| > CVE-2019-3816  |
| > CVE-2021-3750  |
| > CVE-2022-0358  |
| > CVE-2022-26354 |
| > CVE-2022-3165  |
| > CVE-2022-2962  |
| > CVE-2022-41722 |
| > CVE-2022-29526 |
| > CVE-2007-4559  |
| > CVE-2019-9674  |
| > CVE-2017-18207 |
| > CVE-2019-20907 |
| > CVE-2021-23336 |
| > CVE-2017-17522 |
| > CVE-2024-6655  |
| > CVE-2024-2466  |
| > CVE-2024-39331 |
| > CVE-2021-43565 |

|                                  |
|----------------------------------|
| <a href="#">➤ CVE-2024-39277</a> |
| <a href="#">➤ CVE-2024-38780</a> |
| <a href="#">➤ CVE-2024-39292</a> |
| <a href="#">➤ CVE-2024-39482</a> |
| <a href="#">➤ CVE-2024-39484</a> |
| <a href="#">➤ CVE-2024-39495</a> |
| <a href="#">➤ CVE-2024-40902</a> |
| <a href="#">➤ CVE-2024-41110</a> |
| <a href="#">➤ CVE-2024-37298</a> |
| <a href="#">➤ CVE-2024-0397</a>  |
| <a href="#">➤ CVE-2024-38571</a> |
| <a href="#">➤ CVE-2024-42077</a> |
| <a href="#">➤ CVE-2024-39473</a> |
| <a href="#">➤ CVE-2024-26900</a> |
| <a href="#">➤ CVE-2024-39474</a> |
| <a href="#">➤ CVE-2024-42073</a> |
| <a href="#">➤ CVE-2024-42074</a> |
| <a href="#">➤ CVE-2024-42075</a> |
| <a href="#">➤ CVE-2024-42078</a> |
| <a href="#">➤ CVE-2024-0853</a>  |
| <a href="#">➤ CVE-2024-2004</a>  |
| <a href="#">➤ CVE-2024-2398</a>  |
| <a href="#">➤ CVE-2024-38662</a> |

|                                  |
|----------------------------------|
| <a href="#">➤ CVE-2024-36288</a> |
| <a href="#">➤ CVE-2024-39480</a> |
| <a href="#">➤ CVE-2024-39476</a> |
| <a href="#">➤ CVE-2024-39475</a> |
| <a href="#">➤ CVE-2024-37371</a> |
| <a href="#">➤ CVE-2024-26461</a> |
| <a href="#">➤ CVE-2024-37370</a> |
| <a href="#">➤ CVE-2024-6104</a>  |
| <a href="#">➤ CVE-2024-6257</a>  |
| <a href="#">➤ CVE-2024-23722</a> |
| <a href="#">➤ CVE-2024-40898</a> |
| <a href="#">➤ CVE-2024-38583</a> |
| <a href="#">➤ CVE-2024-39493</a> |
| <a href="#">➤ CVE-2024-42068</a> |
| <a href="#">➤ CVE-2024-39489</a> |
| <a href="#">➤ CVE-2024-42070</a> |
| <a href="#">➤ CVE-2024-42076</a> |
| <a href="#">➤ CVE-2024-42080</a> |
| <a href="#">➤ CVE-2024-38428</a> |
| <a href="#">➤ CVE-2024-42082</a> |
| <a href="#">➤ CVE-2022-48788</a> |
| <a href="#">➤ CVE-2023-52340</a> |
| <a href="#">➤ CVE-2022-48841</a> |

|                                  |
|----------------------------------|
| > <a href="#">CVE-2024-39485</a> |
| > <a href="#">CVE-2024-39483</a> |
| > <a href="#">CVE-2024-42071</a> |
| > <a href="#">CVE-2024-42072</a> |
| > <a href="#">CVE-2024-42237</a> |
| > <a href="#">CVE-2024-42083</a> |

CWE's

| CWE                       | Beschrijving                                                                   |
|---------------------------|--------------------------------------------------------------------------------|
| > <a href="#">CWE-115</a> | Misinterpretation of Input                                                     |
| > <a href="#">CWE-119</a> | Improper Restriction of Operations within the Bounds of a Memory Buffer        |
| > <a href="#">CWE-120</a> | Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')         |
| > <a href="#">CWE-122</a> | Heap-based Buffer Overflow                                                     |
| > <a href="#">CWE-125</a> | Out-of-bounds Read                                                             |
| > <a href="#">CWE-129</a> | Improper Validation of Array Index                                             |
| > <a href="#">CWE-187</a> | Partial String Comparison                                                      |
| > <a href="#">CWE-190</a> | Integer Overflow or Wraparound                                                 |
| > <a href="#">CWE-191</a> | Integer Underflow (Wrap or Wraparound)                                         |
| > <a href="#">CWE-193</a> | Off-by-one Error                                                               |
| > <a href="#">CWE-20</a>  | Improper Input Validation                                                      |
| > <a href="#">CWE-22</a>  | Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') |
| > <a href="#">CWE-269</a> | Improper Privilege Management                                                  |
| > <a href="#">CWE-273</a> | Improper Check for Dropped Privileges                                          |
| > <a href="#">CWE-280</a> | Improper Handling of Insufficient Permissions or Privileges                    |

|           |                                                                                                    |
|-----------|----------------------------------------------------------------------------------------------------|
| ➤ CWE-295 | Improper Certificate Validation                                                                    |
| ➤ CWE-297 | Improper Validation of Certificate with Host Mismatch                                              |
| ➤ CWE-299 | Improper Check for Certificate Revocation                                                          |
| ➤ CWE-319 | Cleartext Transmission of Sensitive Information                                                    |
| ➤ CWE-362 | Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')        |
| ➤ CWE-369 | Divide By Zero                                                                                     |
| ➤ CWE-371 | CWE-371                                                                                            |
| ➤ CWE-400 | Uncontrolled Resource Consumption                                                                  |
| ➤ CWE-401 | Missing Release of Memory after Effective Lifetime                                                 |
| ➤ CWE-404 | Improper Resource Shutdown or Release                                                              |
| ➤ CWE-416 | Use After Free                                                                                     |
| ➤ CWE-444 | Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')                   |
| ➤ CWE-476 | NULL Pointer Dereference                                                                           |
| ➤ CWE-532 | Insertion of Sensitive Information into Log File                                                   |
| ➤ CWE-667 | Improper Locking                                                                                   |
| ➤ CWE-74  | Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection') |
| ➤ CWE-77  | Improper Neutralization of Special Elements used in a Command ('Command Injection')                |
| ➤ CWE-770 | Allocation of Resources Without Limits or Throttling                                               |
| ➤ CWE-772 | Missing Release of Resource after Effective Lifetime                                               |
| ➤ CWE-78  | Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')         |
| ➤ CWE-787 | Out-of-bounds Write                                                                                |
| ➤ CWE-833 | Deadlock                                                                                           |
| ➤ CWE-835 | Loop with Unreachable Exit Condition ('Infinite Loop')                                             |

|           |                                                                                        |
|-----------|----------------------------------------------------------------------------------------|
| > CWE-863 | Incorrect Authorization                                                                |
| > CWE-918 | Server-Side Request Forgery (SSRF)                                                     |
| > CWE-94  | Improper Control of Generation of Code ('Code Injection')                              |
| > CWE-95  | Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') |

Getroffen producten

|                  |
|------------------|
| <b>microsoft</b> |
| cbl-mariner      |

Disclaimer

The Netherlands Cyber Security Center (henceforth: NCSC-NL) maintains this page to enhance access to its information and security advisories. The use of this security advisory is subject to the following terms and conditions: NCSC-NL makes every reasonable effort to ensure that the content of this page is kept up to date, and that it is accurate and complete. Nevertheless, NCSC-NL cannot entirely rule out the possibility of errors, and therefore cannot give any warranty in respect of its completeness, accuracy or continuous keeping up-to-date. The information contained in this security advisory is intended solely for the purpose of providing general information to professional users. No rights can be derived from the information provided therein. NCSC-NL and the Kingdom of the Netherlands assume no legal liability or responsibility for any damage resulting from either the use or inability of use of this security advisory. This includes damage resulting from the inaccuracy of incompleteness of the information contained in the advisory. This security advisory is subject to Dutch law. All disputes related to or arising from the use of this advisory will be submitted to the competent court in The Hague. This choice of means also applies to the court in summary proceedings.