Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

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).

Ontvangers van TLP:WHITE mogen de informatie publiek verspreiden.

Uw reacties zijn welkom op 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

- CVE-2024-39277
- CVE-2024-38780
- CVE-2024-39292
- CVE-2024-39482
- CVE-2024-39484
- CVE-2024-39495
- CVE-2024-40902
- CVE-2024-41110
- CVE-2024-37298
- CVE-2024-0397
- CVE-2024-38571
- CVE-2024-42077
- CVE-2024-39473
- CVE-2024-26900
- CVE-2024-39474
- CVE-2024-42073
- CVE-2024-42074
- CVE-2024-42075
- CVE-2024-42078
- CVE-2024-0853
- CVE-2024-2004
- CVE-2024-2398
- CVE-2024-38662

- CVE-2024-36288
- CVE-2024-39480
- CVE-2024-39476
- CVE-2024-39475
- CVE-2024-37371
- CVE-2024-26461
- CVE-2024-37370
- CVE-2024-6104
- CVE-2024-6257
- CVE-2024-23722
- CVE-2024-40898
- CVE-2024-38583
- CVE-2024-39493
- CVE-2024-42068
- CVE-2024-39489
- CVE-2024-42070
- CVE-2024-42076
- CVE-2024-42080
- CVE-2024-38428
- CVE-2024-42082
- CVE-2022-48788
- CVE-2023-52340
- CVE-2022-48841

- CVE-2024-39485
- CVE-2024-39483
- CVE-2024-42071
- CVE-2024-42072
- CVE-2024-42237
- CVE-2024-42083

CWE's

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

microsoft
cbl-mariner

Disclaimer