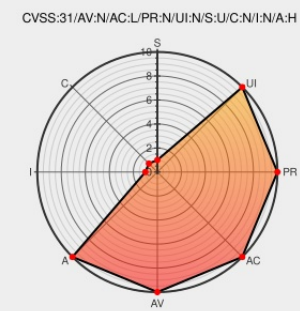
CVE-2022-46770

Published on: Not Yet Published

Last Modified on: 08/08/2023 02:21:00 PM UTC

CVE-2022-46770

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



Certain versions of Mirage Firewall from Linuxfoundation contain the following vulnerability:

qubes-mirage-firewall (aka Mirage firewall for QubesOS) 0.8.x through 0.8.3 allows guest OS users to cause a denial of service (CPU consumption and loss of forwarding) via a crafted multicast UDP packet (IP address range of 224.0.0.0 through 239.255.255.255).

CVE-2022-46770 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Qubes Mirage Firewall 0.8.3 Denial Of Service ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/171610/Qubes-Mirage-Firewall-0.8.3-Denial-Of-Service.html
Mirage v0.8.x DoS from untrusted Qube by sending arbitrary UDP payload · Issue #166 · mirage/qubes-mirage-firewall · GitHub	github.com text/html	MISC github.com/mirage/qubes-mirage-firewall/issues/166

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Linuxfoundation	Mirage Firewall	All	All	All	All

cpe:2.3:a:linuxfoundation:mirage_firewall:*:*:*:*:*:qubesos:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-46770 : qubes-mirage-firewall aka Mirage firewall for QubesOS 0.8.x through 0.8.3 allows guest OS users… twitter.com/i/web/status/1…	2022-12-07 20:05:52
/r/netcve	CVE-2022-46770	2022-12-07 21:41:36
/r/Team_IT_Security	#0daytoday #qubes-mirage-firewall v0.8.3 - Denial Of Service Exploit CVE-2022-46770 [dos #exploits #0day #Exploit]	2023-04-05 21:42:20

← Previous ID

Next ID→