



Advisory NCSC-2026-0452

PRIORITEIT: NORMAAL

Kwetsbaarheden verholpen in FreeBSD bhyve hypervisor

Publicatiedatum: 22-10-2026

Toegestane verspreiding: TLP:WHITE
(Traffic Light Protocol)

Deze publicatie bevat het label TLP:WHITE en wordt door het Nationaal Cyber Security Center (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.

Reacties zijn welkom op info@ncsc.nl.

Feiten

De FreeBSD community heeft meerdere kwetsbaarheden verholpen in bhyve Hypervisor

Duiding

De kwetsbaarheden betreffen race conditions, onjuiste validatie en synchronisatieproblemen in verschillende device modellen binnen de bhyve hypervisor. Een kwaadwillende gast-virtuele machine kan deze fouten misbruiken om een denial of service te veroorzaken door het bhyve proces te laten crashen of om arbitraire code uit te voeren in de host userspace. Dit kan plaatsvinden via manipulatie van event ring size en Transfer Request Block (TRB) velden in de USB 3 device model, het triggeren van out-of-bounds geheugen toegang door onjuiste controle van zero-length Buffer Descriptor List entries in de HDA audio device model, en door het misbruiken van duplicaten, unsynchronized constanten en ontbrekende validatie van resolutieparameters in de framebuffer device model. Deze kwetsbaarheden zijn specifiek voor systemen die de bhyve hypervisor gebruiken.

Oplossingen

FreeBSD heeft updates uitgebracht om deze kwetsbaarheden in de bhyve hypervisor te verhelpen. Zie bijgevoegde referenties voor meer informatie.

Referenties

- <https://security.freebsd.org/advisories/FreeBSD-SA-26:70.tcp.asc>
- <https://security.freebsd.org/advisories/FreeBSD-SA-26:71.sound.asc>
- <https://security.freebsd.org/advisories/FreeBSD-SA-26:72.bhyve.asc>

Kwetsbaarheden

CVE	CVSS Score
CVE-2026-101307	8.2 HIGH
CVE-2026-101308	5.5 MEDIUM
CVE-2026-101309	7.0 HIGH
CVE-2026-101310	7.0 HIGH
CVE-2026-101311	7.0 HIGH

CWE's

CWE	Beschrijving
CWE-122	Heap-based Buffer Overflow
CWE-126	Buffer Over-read
CWE-362	Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')
CWE-367	Time-of-check Time-of-use (TOCTOU) Race Condition
CWE-787	Out-of-bounds Write

Getroffen producten

FreeBSD
FreeBSD

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 or 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.