NVD DB Update

CVE-2022-23087 - Score: 8.8

Components:

freebsd freebsd *
freebsd freebsd 12.3
freebsd freebsd 13.0

Description:

The e1000 network adapters permit a variety of modifications to an Ethernet packet when it is being transmitted. These include the insertion of IP and TCP checksums, insertion of an Ethernet VLAN header, and TCP segmentation offload ("TSO"). The e1000 device model uses an on-stack buffer to generate the modified packet header when simulating these modifications on transmitted packets. When checksum offload is requested for a transmitted packet, the e1000 device model used a guest-provided value to specify the checksum offset in the on-stack buffer. The offset was not validated for certain packet types. A misbehaving bhyve guest could overwrite memory in the bhyve process on the host, possibly leading to code execution in the host context. The bhyve process runs in a Capsicum sandbox, which (depending on the FreeBSD version and bhyve configuration) limits the impact of exploiting this issue.

Main problems:

787 "Out-of-bounds Write"

https://cybersword.tech
www.linkedin.com/in/cybersword-tech
ph1sher
@davidwowa