NVD DB Update

CVE-2023-3494 - Score: 8.8

Components:

freebsd freebsd 13.2
freebsd freebsd 13.1

Description:

The fwctl driver implements a state machine which is executed when a bhyve guest accesses certain x86 I/O ports. The interface lets the guest copy a string into a buffer resident in the bhyve process' memory. A bug in the state machine implementation can result in a buffer overflowing when copying this string. Malicious, privileged software running in a guest VM can exploit the buffer overflow to achieve code execution on the host in the bhyve userspace process, which typically runs as root, mitigated by the capabilities assigned through the Capsicum sandbox available to the bhyve process.

Main problems:

120 "Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')"