-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

```
================================================================================
FreeBSD-SA-26:11.amd64                                        Security Advisory
                                                            The FreeBSD Project

Topic:          Missing large page handling in pmap_pkru_update_range()

Category:       core
Module:         amd64
Announced:      2026-04-21
Credits:        Nicholas Carlini using Claude, Anthropic
Affects:        All supported versions of FreeBSD.
Corrected:      2026-04-21 15:43:03 UTC (stable/15, 15.0-STABLE)
                2026-04-21 15:44:28 UTC (releng/15.0, 15.0-RELEASE-p6)
                2026-04-21 15:43:14 UTC (stable/14, 14.4-STABLE)
                2026-04-21 15:45:32 UTC (releng/14.4, 14.4-RELEASE-p2)
                2026-04-21 15:46:03 UTC (releng/14.3, 14.3-RELEASE-p11)
                2026-04-21 15:43:57 UTC (stable/13, 13.5-STABLE)
                2026-04-21 15:47:08 UTC (releng/13.5, 13.5-RELEASE-p12)
CVE Name:       CVE-2026-6386

For general information regarding FreeBSD Security Advisories,
including descriptions of the fields above, security branches, and the
following sections, please visit <URL:https://security.FreeBSD.org/>.

I.   Background

Memory protection keys are an amd64 CPU feature, available in modern Intel and
AMD CPUs, which allow applications to apply access restrictions to regions of
virtual memory.  On FreeBSD this functionality is provided by the pkru(3)
interface.

II.  Problem Description

In order to apply a particular protection key to an address range, the kernel
must update the corresponding page table entries.  The subroutine which handled
this failed to take into account the presence of 1GB largepage mappings created
using the shm_create_largepage(3) interface.  In particular, it would always
treat a page directory page entry as pointing to another page table page.

III. Impact

The bug can be abused by an unprivileged user to cause pmap_pkru_update_range()
to treat userspace memory as a page table page, and thus overwrite memory to
which the application would otherwise not have access.

IV.  Workaround

No workaround is available.  The bug only affects amd64 systems.

V.   Solution

Upgrade your vulnerable system to a supported FreeBSD stable or
release / security branch (releng) dated after the correction date,
and reboot the system.

Perform one of the following:

1) To update your vulnerable system installed from base system packages:

Systems running a 15.0-RELEASE version of FreeBSD on the amd64 or arm64
platforms, which were installed using base system packages, can be updated
```

via the pkg(8) utility:

```
# pkg upgrade -r FreeBSD-base
# shutdown -r +10min "Rebooting for a security update"
```

2) To update your vulnerable system installed from binary distribution sets:

Systems running a RELEASE version of FreeBSD on the amd64 or arm64 platforms, or the i386 platform on FreeBSD 13, which were not installed using base system packages, can be updated via the freebsd-update(8) utility:

```
# freebsd-update fetch
# freebsd-update install
# shutdown -r +10min "Rebooting for a security update"
```

3) To update your vulnerable system via a source code patch:

The following patches have been verified to apply to the applicable FreeBSD release branches.

a) Download the relevant patch from the location below, and verify the detached PGP signature using your PGP utility.

```
[FreeBSD 15.0]
# fetch https://security.FreeBSD.org/patches/SA-26:11/amd64-15.patch
# fetch https://security.FreeBSD.org/patches/SA-26:11/amd64-15.patch.asc
# gpg --verify amd64-15.patch.asc

[FreeBSD 14.4 and 14.3]
# fetch https://security.FreeBSD.org/patches/SA-26:11/amd64-14.patch
# fetch https://security.FreeBSD.org/patches/SA-26:11/amd64-14.patch.asc
# gpg --verify amd64-14.patch.asc

[FreeBSD 13.5]
# fetch https://security.FreeBSD.org/patches/SA-26:11/amd64-13.patch
# fetch https://security.FreeBSD.org/patches/SA-26:11/amd64-13.patch.asc
# gpg --verify amd64-13.patch.asc
```

b) Apply the patch.  Execute the following commands as root:

```
# cd /usr/src
# patch < /path/to/patch
```

c) Recompile your kernel as described in <URL:https://www.FreeBSD.org/handbook/kernelconfig.html> and reboot the system.

VI.  Correction details

This issue is corrected as of the corresponding Git commit hash in the following stable and release branches:

| Branch/path | Hash | Revision |
|---|---|---|
| stable/15/ | 9331e62e8b80 | stable/15-n283066 |
| releng/15.0/ | 649db49403a7 | releng/15.0-n281023 |
| stable/14/ | 4c0e5e3cc441 | stable/14-n273998 |
| releng/14.4/ | 5787df30dc3e | releng/14.4-n273686 |
| releng/14.3/ | 979e645dd25e | releng/14.3-n271486 |
| stable/13/ | b8fc56193068 | stable/13-n259846 |
| releng/13.5/ | a2f6f2d00125 | releng/13.5-n259211 |

Run the following command to see which files were modified by a particular commit:

```
# git show --stat <commit hash>

Or visit the following URL, replacing NNNNNN with the hash:

<URL:https://cgit.freebsd.org/src/commit/?id=NNNNNN>

To determine the commit count in a working tree (for comparison against
nNNNNNN in the table above), run:

# git rev-list --count --first-parent HEAD

VII. References

<URL:https://www.cve.org/CVERecord?id=CVE-2026-6386>

The latest revision of this advisory is available at
<URL:https://security.FreeBSD.org/advisories/FreeBSD-SA-26:11.amd64.asc>
-----BEGIN PGP SIGNATURE-----

iQIzBAEBCgAdFiEEthUnfoEIffdcgYM7bljekB8AGu8FAmnnoakACgkQbljekB8A
Gu8xHBAA0UShf6OLTcPprJ4YbzORKrmUeN6MPSwrvtn792T01Fi7zXj1IeBd1/N1
25SI2GBhoMWP1wBR9G0Er8Vjv9cn4lnuWCeBIMmaofgLUi/UahT5lLhQGG7e3ypq
DdmfyWwnJ7tAkDvxHUH2t3STjzIsQaH2NSTpxcg5bdSbGSPGr7On2RBKalvLLBon
SUx8FtlOpDj+TttxidoQcYeez8vCkdgn9PCbA/9cxZlFmy+ioE/14PQU2TAYbcnK
mZ3BWOKxRDlBN9zHBwkaSdIgjs6+t0/pCYrlUu2nCaZ9o6dtn/6WtulcuCB/l9DQ
UABsdc2uhCZvafdN316lABxaPLm3+uvcOFqRZs24tkLOYk5JxBYQQdaHrZ4cP+xS
IgQf/Zl5s/ZlwfzOjzTg54KLyH7yxR5iJ/JIJ2mRJ5PZ9wavYGM6czf4l9w+sYQw
wTTQSO/zdLRHgcKUYdq+xpv2AWEkjkZSRxRQhgMZ9rS5V+1MqhnCLs9uCsG/Ns7c
Yv7t8I+r7j3gjdEFJRDVW+awHQR2ppI/odmyABaThG3bBdPxXy9pR0IvSYtZKGEW
cUjYp2intHCDna0TSa4nzrTlCZCAZijVKeVLXSrYNvrJ9nE3dB8oESP2YASjyJBM
VxpRYXmjprazBYcRgt7kf/tSfpky7Cq59H1NU+pVxaR5TAzWvaI=
=kWUu
-----END PGP SIGNATURE-----
```