```
=============================================================================
FreeBSD-SA-18:03.speculative_execution                      Security Advisory
                                                          The FreeBSD Project

Topic:          Speculative Execution Vulnerabilities

Category:       core
Module:         kernel
Announced:      2018-03-14
Credits:        Jann Horn (Google Project Zero); Werner Haas, Thomas
                Prescher (Cyberus Technology); Daniel Gruss, Moritz Lipp,
                Stefan Mangard, Michael Schwarz (Graz University of
                Technology); Paul Kocher; Daniel Genkin (University of
                Pennsylvania and University of Maryland), Mike Hamburg
                (Rambus); Yuval Yarom (University of Adelaide and Data6)
Affects:        All supported versions of FreeBSD.
Corrected:      2018-02-17 18:00:01 UTC (stable/11, 11.1-STABLE)
                2018-03-14 04:00:00 UTC (releng/11.1, 11.1-RELEASE-p8)
CVE Name:       CVE-2017-5715, CVE-2017-5754

Special Note:   Speculative execution vulnerability mitigation is a work
                in progress.  This advisory addresses the most significant
                issues for FreeBSD 11.1 on amd64 CPUs.  We expect to update
                this advisory to include 10.x for amd64 CPUs.  Future FreeBSD
                releases will address this issue on i386 and other CPUs.
                freebsd-update will include changes on i386 as part of this
                update due to common code changes shared between amd64 and
                i386, however it contains no functional changes for i386 (in
                particular, it does not mitigate the issue on i386).

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

Many modern processors have implementation issues that allow unprivileged
attackers to bypass user-kernel or inter-process memory access restrictions
by exploiting speculative execution and shared resources (for example,
caches).

II.  Problem Description

A number of issues relating to speculative execution were found last year
and publicly announced January 3rd.  Two of these, known as Meltdown and
Spectre V2, are addressed here.

CVE-2017-5754 (Meltdown)
- ------------------------

This issue relies on an affected CPU speculatively executing instructions
beyond a faulting instruction.  When this happens, changes to architectural
state are not committed, but observable changes may be left in micro-
architectural state (for example, cache).  This may be used to infer
privileged data.

CVE-2017-5715 (Spectre V2)
- --------------------------

Spectre V2 uses branch target injection to speculatively execute kernel code
at an address under the control of an attacker.
```

III. Impact

An attacker may be able to read secret data from the kernel or from a
process when executing untrusted code (for example, in a web browser).

IV. Workaround

No workaround is available.

V.   Solution

Perform one of the following:

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

2) To update your vulnerable system via a binary patch:

Systems running a RELEASE version of FreeBSD on the i386 or amd64
platforms can be updated via the freebsd-update(8) utility, followed
by a reboot into the new kernel:

```
# freebsd-update fetch
# freebsd-update install
# shutdown -r now
```

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 11.1]
# fetch https://security.FreeBSD.org/patches/SA-18:03/speculative_execution-amd64-11.patch
# fetch https://security.FreeBSD.org/patches/SA-18:03/speculative_execution-amd64-
11.patch.asc
# gpg --verify speculative_execution-amd64-11.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

CVE-2017-5754 (Meltdown)
- ------------------------

The mitigation is known as Page Table Isolation (PTI). PTI largely separates
kernel and user mode page tables, so that even during speculative execution
most of the kernel's data is unmapped and not accessible.

A demonstration of the Meltdown vulnerability is available at
https://github.com/dag-erling/meltdown. A positive result is definitive
(that is, the vulnerability exists with certainty). A negative result
indicates either that the CPU is not affected, or that the test is not
capable of demonstrating the issue on the CPU (and may need to be modified).

A patched kernel will automatically enable PTI on Intel CPUs. The status can be checked via the vm.pmap.pti sysctl:

```
# sysctl vm.pmap.pti
vm.pmap.pti: 1
```

The default setting can be overridden by setting the loader tunable vm.pmap.pti to 1 or 0 in /boot/loader.conf. This setting takes effect only at boot.

PTI introduces a performance regression. The observed performance loss is significant in microbenchmarks of system call overhead, but is much smaller for many real workloads.

CVE-2017-5715 (Spectre V2)

There are two common mitigations for Spectre V2. This patch includes a mitigation using Indirect Branch Restricted Speculation, a feature available via a microcode update from processor manufacturers. The alternate mitigation, Retpoline, is a feature available in newer compilers. The feasibility of applying Retpoline to stable branches and/or releases is under investigation.

The patch includes the IBRS mitigation for Spectre V2. To use the mitigation the system must have an updated microcode; with older microcode a patched kernel will function without the mitigation.

IBRS can be disabled via the hw.ibrs_disable sysctl (and tunable), and the status can be checked via the hw.ibrs_active sysctl. IBRS may be enabled or disabled at runtime. Additional detail on microcode updates will follow.

The following list contains the correction revision numbers for each affected branch.

Branch/path	Revision
stable/11/	r329462
releng/11.1/	r330908

To see which files were modified by a particular revision, run the following command, replacing NNNNNN with the revision number, on a machine with Subversion installed:

```
# svn diff -cNNNNNN --summarize svn://svn.freebsd.org/base
```

Or visit the following URL, replacing NNNNNN with the revision number:

<URL:https://svnweb.freebsd.org/base?view=revision&revision=NNNNNN>

VII. References

<URL:https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5715>

<URL:https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5754>

The latest revision of this advisory is available at
<URL:https://security.FreeBSD.org/advisories/FreeBSD-SA-18:03.speculative_execution.asc>

-----BEGIN PGP SIGNATURE-----

iQKTBAEBCgB9FiEE/A6HiuWv54gCjWNV05eS9J6n5cIFAlqon0RfFIAAAAAALgAo
aXNzdWVyLWZwckBub3RhdGlvbnMub3BlbnBncC5maWZ0aGhvcnNlbWFuLm5ldEZD
MEU4NzhBRTVBRkU3ODgwMjhENjM1NUQzOTc5MkY0OUVBN0U1QzIACgkQ05eS9J6n

```
5cKORw/+Lc5lxLhDgU1rQ0JF6sb2b80Ly5k+rJLXFWBvmEQt0uVyVkF4TMJ99M04
bcmrLbT4Pl0Csh/iEYvZQ4el12KvPDApHszsLTBgChD+KfCLvCZvBZzasgDWGD0E
JhL4eIX0wjJ4oGGsT+TAqkmwXyAMJgWW/ZgZPFVXocylZTL3fV4g52VdG1Jnd2yu
hnkViH2kVlVJqXX9AHlenIUfEmUiRUGrMh5oPPpFYDDmfJ+enZ8QLxfZtOKIliD7
u+2GP8V/bvaErkxqF5wwobybrBOMXpq9Y/fWw0EH/om7myevj/oORqK+ZmGZ17bl
IRbdWxgjc1hN2TIMVn9q9xX6i0I0wSPwbpLYagKnSnE8WNVUTZUteaj1GKGTG1rj
DFH2zOLlbRr/IXUFldM9b6VbZX6G5Ijxwy1DJzB/0KL5ZTbAReUR0pqHR7xpulbJ
eDv8SKCwYiUpMuwPOXNdVlVLZSsH5/9A0cyjH3+E+eIhM8qyxw7iRFwA0DxnGVkr
tkMo51Vl3Gl7JFFimGKljsE9mBh00m8B0WYJwknvfhdehO4WripcwI7/V5zL6cwj
s018kaW4Xm77LOz6P1iN8nbcjZ9gN2AsPYUYYZqJxjCcZ7r489Hg9BhbDf0QtC0R
gnwZWiZ/KuAy0C6vaHljsm0xPEM5nBz/yScFXDbuhEdmEgBBD6w=
=fqrI
-----END PGP SIGNATURE-----
```