[<prev] [next>] [day] [month] [year] [list]

Date: Thu, 10 Jun 2021 09:16:42 +0000
From: Xen.org security team <security@....org>
To: xen-announce@...ts.xen.org, xen-devel@...ts.xen.org,
 xen-users@...ts.xen.org, oss-security@...ts.openwall.com
CC: Xen.org security team <security-team-members@....org>
Subject: Xen Security Advisory 375 v4 (CVE-2021-0089,CVE-2021-26313) -
 Speculative Code Store Bypass

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Xen Security Advisory CVE-2021-0089,CVE-2021-26313 / XSA-375
version 4

Speculative Code Store Bypass

UPDATES IN VERSION 4

Correct the link to the AMD bulletin.

ISSUE DESCRIPTION

Modern superscalar processors may employ sophisticated decoding and caching of the instruction stream to improve performance. However, a consequence is that self-modifying code updates may not take effect instantly.

Whatever the architectural guarantees, some CPUs have microarchitectural behaviour whereby the stale instruction stream may be speculatively decoded and executed.

Speculation of this form can suffer from type confusion in registers, and potentially leak data.

For more details, see:
  https://www.vusec.net/projects/fpvi-scsb
  https://www.amd.com/en/corporate/product-security/bulletin/amd-sb-1003
  https://software.intel.com/content/www/us/en/develop/articles/software-security-guidance/advisory-guidance/speculative-code-store-bypass.html
  https://software.intel.com/content/www/us/en/develop/articles/software-security-guidance/advisory-guidance/floating-point-value-injection.html
  https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability/frequently-asked-questions#scsb
  https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability/frequently-asked-questions#fvpi

IMPACT

In attacker might be able to infer the contents of arbitrary host memory, including memory assigned to other guests.

VULNERABLE SYSTEMS

Systems running all versions of Xen are affected.

Whether a CPU is potentially vulnerable depends on its microarchitecture. Consult your hardware vendor.

Xen running on ARM does not have runtime self-modying code, so is believed to be not vulnerable, irrespective of any hardware susceptibility.

Xen running on x86 does have runtime self-modying code as part of emulation, and is believed to be potentially vulnerable.

Xen is not vulnerable if retpoline or lfence mitigations for Spectre v2 protection are active. Protections depend on compiler support (as indicated by INDIRECT_THUNK), and a runtime setting (BTI-Thunk):

```
  # xl dmesg | grep -e INDIRECT_THUNK -e BTI-Thunk
  (XEN)   Compiled-in support: INDIRECT_THUNK SHADOW_PAGING
  (XEN)   Xen settings: BTI-Thunk RETPOLINE, SPEC_CTRL: IBRS+ SSBD-, Other: SRB_LOCK+ IBPB L1D_FLUSH VERW BRANCH_HARDEN
```

BTI-Thunk as either RETPOLINE or LFENCE prevents the vulnerability.

MITIGATION

If Spectre v2 support is compiled in, but JMP is used by default, RETPOLINE or LFENCE can be selected with `spec-ctrl=bti-thunk=retpoline` or `spec-ctrl=bti-thunk=lfence`.

CREDITS

This issue was discovered by Enrico Barberis, Hany Ragab, Herbert Bos, and Cristiano Giuffrida from the VUSec group at VU Amsterdam.

RESOLUTION

Applying the appropriate attached patch resolves this issue. Note that in 4.13 and newer the patch will only take effect when the SPECULATIVE_HARDEN_BRANCH hypervisor config option is enabled. 4.12 and older do not have such an option, and the change will take effect unconditionally.

Note that patches for released versions are generally prepared to apply to the stable branches, and may not apply cleanly to the most recent release tarball. Downstreams are encouraged to update to the tip of the stable branch before applying these patches.

xsa375.patch	xen-unstable - 4.14.x
xsa375-4.13.patch	Xen 4.13.x
xsa375-4.12.patch	Xen 4.12.x - 4.11.x

```
$ sha256sum xsa375*
367d5bb97c942b9f744a57645df87148772c0879de6f351f36f88147f3958e83  xsa375.meta
301ef80da837bc2af36a0958f35f42f4d267b20ec6e91ae5faf2616167ef49f8  xsa375.patch
dc024daf17242b6477a16a349754a94b2b25cbbfd8c14475741b778710a44c93  xsa375-4.12.patch
f70511d843c6617b932da11ffe857e2e3aa3834ccff07d4d0beba90d63a3dae2  xsa375-4.13.patch
$
```

NOTE CONCERNING CVE-2021-0086 / CVE-2021-26314

Floating Point Value Injection (FPVI) was discovered and disclosed in the same research as SCSB. Xen on x86 does in some cases emulate floating point operations with guest provided inputs, but does not have subsequent control flow dependent on results, transient or otherwise, of the operation.

Therefore, we believe Xen is not vulnerable to FPVI, irrespective of any hardware susceptibility.

NOTE CONCERNING MULTIPLE CVES

Intel and AMD allocated different CVEs for SCSB and FPVI. We have included both on this advisory. The allocations are as follows:

Issue	Intel	AMD
SCSB	CVE-2021-0089	CVE-2021-26313
FPVI	CVE-2021-0086	CVE-2021-26314

DEPLOYMENT DURING EMBARGO

Deployment of the patches and/or mitigations described above (or others which are substantially similar) is permitted during the embargo, even on public-facing systems with untrusted guest users and administrators.

But: Distribution of updated software is prohibited (except to other members of the predisclosure list).

Predisclosure list members who wish to deploy significantly different patches and/or mitigations, please contact the Xen Project Security Team.

(Note: this during-embargo deployment notice is retained in post-embargo publicly released Xen Project advisories, even though it is then no longer applicable. This is to enable the community to have oversight of the Xen Project Security Team's decisionmaking.)

For more information about permissible uses of embargoed information, consult the Xen Project community's agreed Security Policy:
  http://www.xenproject.org/security-policy.html

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

iQFABAEBCAAqFiEEI+MiLBRfRHX6gGCng/4UyVfoK9kFAmDB2EQMHHBncEB4ZW4u
b3JnAAoJEIP+FMlX6CvZtgkIAMJ6zrjSMK/mrnJ8+vRwfaG7hYIOwIa8k18CnIin
DH4LZ1PIyWRqOjgRo+oqgZEIOXFAlEx/ZXHJscf+SaleemA9klsBWpoiyURONchC
4Sz/qUcJnTHXjakw21seaxtYA4FzBtGQ6V/Ccm/3vDxVhDewtbNSJLflq2kZDLv0
nRMJkSajeCml/YPcSQ2y32KE49kQK726H9hzHIMuRA6fDAKCT51bWiyelH405vnR
vanJetUHys1Uye0arqfi7Z9tv0KMKAspgR/ccOGh5g0EvDOTyOo6ZLAOm69wqdfr
AC0IShNIPyk85k1VJBkU8VSsWvasPmbcT9NYWK6HeP6ZdRg=
=T+nf
-----END PGP SIGNATURE-----
```

Download attachment "xsa375.meta**" of type "**application/octet-stream**" (1821 bytes)**

Download attachment "xsa375.patch**" of type "**application/octet-stream**" (2467 bytes)**

Download attachment "xsa375-4.12.patch**" of type "**application/octet-stream**" (2492 bytes)**

Download attachment "xsa375-4.13.patch**" of type "**application/octet-stream**" (2473 bytes)**