Information

Advisory	XSA-316
Public release	2020-04-14 12:00
Updated	2020-04-14 12:00
Version	3
CVE(s)	CVE-2020-11743
Title	Bad error path in GNTTABOP_map_grant

Files

advisory-316.txt (signed advisory file)
xsa316/xsa316-linux.patch
xsa316/xsa316-xen.patch

Advisory

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

            Xen Security Advisory CVE-2020-11743 / XSA-316
                               version 3

                 Bad error path in GNTTABOP_map_grant

UPDATES IN VERSION 3
====================

Public release.

ISSUE DESCRIPTION
=================

Grant table operations are expected to return 0 for success, and a
negative number for errors.  Some misplaced brackets cause one error
path to return 1 instead of a negative value.

The grant table code in Linux treats this condition as success, and
proceeds with incorrectly initialised state.

IMPACT
======

A buggy or malicious guest can construct its grant table in such a way
that, when a backend domain tries to map a grant, it hits the incorrect
error path.

This will crash a Linux based dom0 or backend domain.

VULNERABLE SYSTEMS
==================

Systems running any version of Xen with the XSA-295 fixes are
vulnerable.  Systems which have not yet taken the XSA-295 fixes are not
vulnerable.

Systems running a Linux based dom0 or driver domain are vulnerable.

Systems running a FreeBSD or NetBSD based dom0 or driver domain are not
impacted, as they both treat any nonzero value as a failure.

The vulnerability of other systems will depend on how they behave when
getting an unexpected positive number from the GNTTABOP_map_grant
hypercall.

MITIGATION
==========

Applying the Linux patches alone is sufficient to mitigate the issue.
This might be a preferred route for downstreams who support livepatching
Linux but not Xen.

CREDITS
=======

This issue was discovered by Ross Lagerwall of Citrix.

RESOLUTION
==========

Applying the appropriate Xen patch will resolve this issue.

Additionally, a Linux patch is provided to make Linux's behaviour more
robust to unexpected values.

We recommend taking both patches if at all possible.

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.

xsa316/xsa316-xen.patch       Xen 4.9 - xen-unstable
xsa316/xsa316-linux.patch     Linux

$ sha256sum xsa316*/*
7dcd02e8cc0434046747d572bc6c77cd3a2e4041eefd2fa703f4130e998b58dd  xsa316/xsa316-linux.patch
4007578e30730861750d8808c0b63f2e03bbb05df909d71de1920108481 6a8b9  xsa316/xsa316-xen.patch
$

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/4UyVfoK9kFAl6Vpd0MHHBncEB4ZW4u
b3JnAAoJEIP+FMlX6CvZjOgH/lxKsvqDnR04knl9OWvgL690gqxZpwliRRDwwkWh
lkOHJq2jsvm5bq38fYY9WpvmtvHW/RoM53KacyzlRl0y9VvK6hDU7P5np4WkMueX
iEJOcIbQaulPg8/zD8hYkqNNGTCjb79ZhggTihlHxpeZJTa7TJv9bNsZpCQkw+P/
EBXpfsqoPqAMNlqt5PclCT5zlasyBUVjW6+lF3tF6q77knQoWNpKbIOSqL2/V2/p
vUMP/qyUikWW8JLH8N48jpRmFzjxwoDI4/3ElsbSv2VxlX1FksbZxanlcwcjoSG6
004GYSxqOjP4oPEAOrC6sXxc6DKoLLa8SVzYNhkg3XoScY0=
=qCJA
-----END PGP SIGNATURE-----
```

Xenproject.org Security Team