OpenStack Documentation

Contents

Affects
Description
Patches
Credits
References
Notes

OSSA-2025-001: Ironic fails to restrict paths used for file:// image URLs

Date: May 08, 2024
CVE: CVE-2025-44021

Affects

- Ironic: <24.1.3, >=25.0.0 <26.1.1, >=27.0.0, <29.0.1

Description

Julia Kreger of Red Hat noticed a vulnerability in image handling for Ironic. A malicious project assigned as a node owner can provide a path to any local file readable by the ironic-conductor which may then be written to the target node disk. This is only possible via deployments performed directly via Ironic's API and cannot be triggered via Nova's virt driver.

This is difficult to exploit in practice, as a node deployed in this manner should not ever reach ACTIVE state, but it still represents a danger in environments running with non-default, insecure configurations such as with automated cleaning disabled.

Patches

- https://review.opendev.org/c/openstack/ironic/+/949175 (2024.1/caracal)
- https://review.opendev.org/c/openstack/ironic/+/949174 (2024.2/dalmatian)
- https://review.opendev.org/c/openstack/ironic/+/949173 (2025.1/epoxy)
- Patch attached to https://bugs.launchpad.net/ironic/+bug/2107847/comments/47 (Bobcat/2023.2-eol)

- https://review.opendev.org/c/openstack/ironic/+/949186 (Bugfix/26.0)
- https://review.opendev.org/c/openstack/ironic/+/949185 (Bugfix/27.0)
- https://review.opendev.org/c/openstack/ironic/+/949184 (Bugfix/28.0)
- https://review.opendev.org/c/openstack/ironic/+/949172 (Master)
- https://review.opendev.org/c/openstack/ironic/+/949182 (Unmaintained/2023.1 antelope)
- https://review.opendev.org/c/openstack/ironic/+/949179 (Unmaintained/xena)
- https://review.opendev.org/c/openstack/ironic/+/949177 (Unmaintained/yoga)
- https://review.opendev.org/c/openstack/ironic/+/949176 (Unmaintained/zed)

Credits

- Julia Kreger from Red Hat (C, V, E, -, 2, 0, 2, 5, -, 4, 4, 0, 2, 1)

References

- https://launchpad.net/bugs/2107847
- http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-44021

Notes

- Patches have been provided for all supported Ironic branches. As a courtesy, we have also provided patches for some unmaintained branches and the recently end-of-life 2023.2/bobcat release. As usual, we will provide updated releases off maintained branches, but will not create new releases off bugfix or unmaintained branches.