Researchers Detail Privilege Escalation Bugs Reported in Oracle VirtualBox [2]

A now-patched vulnerability affecting Oracle VM VirtualBox could be potentially exploited by an adversary to compromise the hypervisor and cause a denial-of-service (DoS) condition.

"Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle VM VirtualBox executes to compromise Oracle VM VirtualBox," the advisory reads. "Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DoS) of Oracle VM VirtualBox"


Single Sign-On and zero trust networks depend on securely passing identification details back and forth between users, identity providers, and service providers. SAML is the glue that lets that happen.

Security updates for Thursday [4]

Security updates have been issued by Fedora (busybox, getdata, and php), Mageia (couchdb, freerdp, openexr, postgresql, python-reportlab, and rsh), openSUSE (bind, java-1_8_0-openjdk, and kernel), SUSE (java-1_7_0-openjdk), and Ubuntu (icu).
International Organization for Standardization (ISO) developed the OSI model in 1984.

OSI model is an acronym for Open System Interconnect.

The OSI model is a model that allows us to categorize network communications and divide different activities of the network in seven conceptual layers. This model tries to explain how the data of an application passes through the device and out in the physical network using the seven conceptual steps or layers.

In simpler words, it explains how one application performs different steps to communicate its data to another application running on a different device.

The OSI model was created for creating a common industry standard, which could have helped inter-operability between different vendors.

However, this model did not gain a lot of popularity. So it is used as a reference or a teaching tool today. The OSI model does not directly match the networking systems we use in reality, but it is still useful because it describes the several processes used in electronic communication.

New Linux malware hides in cron jobs with invalid dates [6] [Ed: This is not a "Linux" issue; it's about applications that run over the Web and have holes in them, maybe because admins do not patch them]

Security researchers have discovered a new remote access trojan (RAT) for Linux that keeps an almost invisible profile by hiding in tasks scheduled for execution on a non-existent day, February 31st.

Dubbed CronRAT, the malware is currently targeting web stores and enables attackers to steal credit card data by deploying online payment skimmers on Linux servers.

Security

Source URL: http://www.tuxmachines.org/node/158376

Links:
[4] https://lwn.net/Articles/876852/rss