[CVE-2022-32224] Possible RCE escalation bug with Serialized Columns in Active Record

2814 views

Aaron Patterson Jul 12, 2022, 5:36:52 PM

to ruby-sec...@googlegroups.com, rubyonrail...@googlegroups.com

There is a possible escalation to RCE when using YAML serialized columns in Active Record. This vulnerability has been assigned the CVE identifier CVE-2022-32224.

Versions Affected: All.
Not affected: None
Fixed Versions: 7.0.3.1, 6.1.6.1, 6.0.5.1, 5.2.8.1

Impact

When serialized columns that use YAML (the default) are deserialized, Rails uses `YAML.unsafe_load` to convert the YAML data in to Ruby objects. If an attacker can manipulate data in the database (via means like SQL injection), then it may be possible for the attacker to escalate to an RCE.

Impacted Active Record models will look something like this: