Main page
Recent changes
Server admin log (Prod)
Server admin log (RelEng)
Deployments
SRE/Operations Help
Incident status

Cloud VPS & Toolforge
Cloud VPS documentation
Toolforge documentation
Request Cloud VPS project
Server admin log (Cloud VPS)

Tools
What links here
Related changes
Special pages
Permanent link
Page information
Cite this page

Print/export
Create a book
Download as PDF
Printable version

Incident documentation/20160212-LabsSudoVulnerability

< Incident documentation

Summary

From 2016-02-12 through 2016-02-21, all labs instances had a lax 'run anything as anyone' sudo policy in place. Chase and Andrew audited instances of concern, and found a very small number of suspicious sudo uses on tools-bastion-01. That instance is currently turned off and has been replaced by a new scratch-built bastion host.

The pre-February-12th sudo policies are now back in place.

Timeline

- [2016-02-12] As part of migrating projects to keystone each Labs project was recreated with the new keystone-aware code. This had the accidental side-effect of re-applying the default sudo policies to each product, which allowed global sudo and sudo-as.
- [2016-02-21] The insecurity problem was discovered by labs volunteer 'Southparkfan' and communicated to Coren and Andrew discreetly. The cause of the problem was immediately apparent. Andrew temporarily removed all global sudo rules across labs. Andrew then located a dump of the sudo rules from late December and generated a list of projects that had restricted sudo before 2016-02-12; standardized, permissive sudo rules were re-applied to all other projects a few hours later using an ad-hoc wikitech maintenance script.

Meanwhile, Chase inspected the auth logs on all instaces in the affect projects:

```
hostname -f && zgrep sudo: /var/log/auth.log*| grep 'PWD='| egrep -v 'USER=
(puppet|tools.)'|grep -v '  diamond : '" >> $p.authlog
for f in `ls *.authlog`; do cat $f | awk '{print $6,$14}' | sort | uniq >
$f.sudoers; done
```

There were a few suspicious lines in the logs for tools-bastion-01, so Andrew shutdown that instance and directed tools bastion traffic to tools-bastion-02.

Toollabs users were informed of the potential breach and encouraged to rotate passwords. While troubleshooting was in progress, the issue was tracked in https://phabricator.wikimedia.org/T127656.

- [2016-02-22] Andrew builds and provisions tools-bastion-05 as a complete replacement for tools-bastion-01.

Affected projects

The following projects had elevated sudo access between the 12th and the 21st:

'catgraph', 'translatesvg', 'toolsbeta', 'jawiki', 'wmve-techteam', 'utrs', 'wmt', 'bastion', 'project-proxy', 'mediawiki-verp', 'glam', 'wlmjudging', 'tools', 'account-creation-assistance'

Conclusions

The ldap->keystone migration that caused this problem was quite complicated; all migration code was extensively tested and reviewed. Nonetheless, this error is a repeat of one made in a different outage: specifically, testing focused more on positive "can I do what I should be able to" testing vs. "am I prevented from doing what I should not be able to do" testing.

Since auth.logs are stored on the affected systems, there's no way to be positive that systems were not compromised. Fortunately, most access rules (both for logins and sudo) are managed from outside of labs instances, so it's unlikely that any exploits persisted after the sudo policies were updated.

Actionables

- Write some labs tests that monitor login and sudo permissions
- Move labs auth.logs to central logging

The necessary changes to close the potential exploit are complete, as are most possible audits and inspections.

Category: Incident documentation