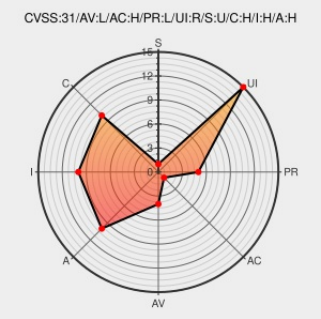
CVE-2020-8903

Published on: 06/22/2020 12:00:00 AM UTC

Last Modified on: 09/30/2022 11:06:00 PM UTC

CVE-2020-8903

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Guest-oslogin from Google contain the following vulnerability:

A vulnerability in Google Cloud Platform's guest-oslogin versions between 20190304 and 20200507 allows a user that is only granted the role "roles/compute.osLogin" to escalate privileges to root. Using their membership to the "adm" group, users with this role are able to read the DHCP XID from the systemd journal. Using the DHCP XID, it is then possible to set the IP address and hostname of the instance to any value, which is then stored in /etc/hosts. An attacker can then point metadata.google.internal to an arbitrary IP address and impersonate the GCE metadata server which make it is possible to instruct the OS Login PAM module to grant administrative privileges. All images created after 2020-May-07 (20200507) are fixed, and if you cannot update, we recommend you edit /etc/group/security.conf and remove the "adm" user from the OS Login entry.

CVE-2020-8903 has been assigned by security@google.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Google LLC** - **guest-oslogin** version **>= 20190304**

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	LOW	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6.9 - MEDIUM

Access Vector	Access Complexity	Authentication
LOCAL	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**

COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
[security-announce] openSUSE-SU-2020:1014-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:1014
oslogin-privesc-june-2020 · master · GitLab.com / GitLab Security Department / GitLab Red Team / Red Team Tech Notes · GitLab	Exploit Third Party Advisory gitlab.com text/html	MISC gitlab.com/gitlab-com/gl-security/gl-redteam/red-team-tech-notes/-/tree/master/oslogin-privesc-june-2020
Google Cloud Platform Security Bulletins | Support	Vendor Advisory cloud.google.com text/html	MISC cloud.google.com/support/bulletins/#gcp-2020-008
Remove OS Login users from admin groups. by illfelder · Pull Request #29 · GoogleCloudPlatform/guest-oslogin · GitHub	Patch Third Party Advisory github.com text/html	CONFIRM github.com/GoogleCloudPlatform/guest-oslogin/pull/29
[security-announce] openSUSE-SU-2020:0996-1: important: Security update	lists.opensuse.org text/html	SUSE openSUSE-SU-2020:0996

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Google	Guest-oslogin	All	All	All	All
Operating System	Opensuse	Leap	15.1	All	All	All
Operating System	Opensuse	Leap	15.2	All	All	All

cpe:2.3:a:google:guest-oslogin:*:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:15.1:*:*:*:*:*:*:*:

cpe:2.3:o:opensuse:leap:15.2:*:*:*:*:*:*:*:

Discovery Credit

Chris Moberly

Social Mentions

Source	Title	Posted (UTC)

Source	Title	Posted (UTC)

← Previous ID

Next ID→