



Advisory Alert

Alert Number: AAA20210127

Date: January 27, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	High	Buffer Overflow
Apache Guacamole	High	Information Disclosure

Description

Affected Product	Redhat
Severity	High
Affected Vulnerability	Buffer Overflow (CVE-2021-3156)
Description	A heap-based buffer overflow was found in the way sudo parses command line arguments. This vulnerability is exploitable by any local user such as normal users and system users, sudoers and non-sudoers without authentication. Any successful exploitation of this flaw could lead to privilege escalation. It's has highest threat is data confidentiality and system availability.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/security/cve/CVE-2021-3156

Affected Product	Apache Guacamole
Severity	High
Affected Vulnerability	Information Disclosure (CVE-2020-11997)
Description	Apache Guacamole vulnerable versions do not always restrict access to connection history based on user visibility. Some multiple users share access to the same connection, those user connections may be able to see which other users have accessed. Such as IP addresses from which that connection was accessed
Affected Products	Apache Guacamole 1.2.0 and earlier
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://guacamole.apache.org/security/

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.

Financial Sector Computer Security Incident Response Team (FinCSIRT)

LankaClear Pvt Ltd, Level 18, Bank of Ceylon Head Office, BOC Square, 01 Bank of Ceylon Mawatha, Colombo 00100, Sri Lanka

Hotline: + 94 112039777