

Product Security Advisory

November 30, 2021

JCI-PSA-2021-20
CVE-2021-3156
ICSA-21-334-04



Overview

Earlier this year a vulnerability was identified in the Linux package “sudo”. AC2000 from CEM Systems, an enterprise access control and integrated security management system, uses the Linux operating system and is affected by this “sudo” vulnerability. The “sudo” package controls the provisioning of super user (administrator) access to the operating system.

Impact

Under specific circumstances, a local user could use this issue to obtain super user access to the underlying Linux operating system.

Affected Versions

- This affects all versions of AC2000 prior to version 10.6.

Mitigation

- Johnson Controls recommends that customers, with AC2000 versions prior to 10.6, simply remove sudo. To do this, customers may either contact their CEM support team:
<https://www.cemsys.com/support/technical-helpdesk>
or simply login to their Linux servers as root and type **rpm -e sudo**

Note: AC2000 v10.6 includes a fixed version of sudo

Initial Publication Date

November 30, 2021

Last Published Date

November 30, 2021

Resources

Cyber Solutions Website - <https://www.johnsoncontrols.com/cyber-solutions/security-advisories>
CVE-2021-3156 - [NIST National Vulnerability Database \(NVD\)](#) and [MITRE CVE® List](#)
ICSA-21-334-04 - [CISA ICS-CERT Advisories](#)