Security Bulletin

SecB0005: CVE-2021-4034 Polkit's pkexec utility vulnerability

Summary

First published: February 2, 2022

Description	A local privilege escalation vulnerability was found on polkit's pkexec utility. The pkexec application is a setuid tool designed to allow unprivileged users to run commands as privileged users according to predefined policies. The current version of pkexec doesn't handle the calling parameters count correctly and ends trying to execute environment variables as commands. An attacker can leverage this by crafting environment variables in such a way it'll induce pkexec to execute arbitrary code. When successfully executed the attack can cause a local privilege escalation given unprivileged users administrative rights on the target machine.
Affected Products	CopperCube
Recommended Action	Enable firewall protection
CVSS v3.0 Base Score	7.8 High
CVE ID	CVE-2021-4034

Description

A local privilege escalation vulnerability was found on polkit's pkexec utility. The pkexec application is a setuid tool designed to allow unprivileged users to run commands as privileged users according to predefined policies. The current version of pkexec doesn't handle the calling parameters count correctly and ends trying to execute environment variables as commands. An attacker can leverage this by crafting environment variables in such a way it'll induce pkexec to execute arbitrary code. When successfully executed the attack can cause a local privilege escalation given unprivileged users administrative rights on the target machine.

Security Bulletin

Recommended Action

While the CopperCube includes an internal firewall by default, we strongly recommend having an IT-managed firewall on the overall building network if security is a concern.

Although the CVSS base score on CVE-202-4034 is High, this vulnerability has been mitigated. Each CopperCube is protected by a unique randomized strong password. Only authorized Delta Controls personnel have access to SSH passwords. Therefore, the risk has been reduced to Low.

Delta Controls' cloud-based archiver enteliVAULT can be used as an alternative to CopperCube. An on-premises version of enteliVAULT is currently in development with a scheduled release date of April 2022.

17850 56 Ave Surrey BC Canada V3C 1C7 | Tel: 604.574.9444 | deltacontrols.com

Security Bulletin

Appendix: About CVSS

All CVSS scores can be mapped to the qualitative ratings defined by the Qualitative Severity Rating Scale table (see below):

Rating	CVSS Score
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

The Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and severity of software vulnerabilities. CVSS consists of three metric groups: Base, Temporal, and Environmental. The Base group represents the intrinsic qualities of a vulnerability that are constant over time and across user environments. The Base group is composed of two sets of metrics: the Exploitability metrics and the Impact metrics.

- The Exploitability metrics reflect the ease and technical means by which the vulnerability can be exploited. That is, they represent characteristics of the thing that is vulnerable, which we refer to formally as the vulnerable component. On the other hand, the Impact metrics reflect the direct consequence of a successful exploit and represent the consequence to the thing that suffers the impact, which we refer to formally as the impacted component.
- The CVSS v3.0 vector string is a text representation of a set of CVSS metrics. It is commonly used to record or transfer CVSS metric information in a concise form.

For more information, visit the CVSS website at: http://www.first.org/cvss/