MNDT-2022-0028

Description

Mandiant consultants discovered a vulnerability that impacts eG Innovations' eG Agent product, allowing a low privileged user to elevate privileges on systems where eG Agent is installed in its default configuration.

Impact

High - An attacker can abuse this vulnerability to elevate privileges on the affected system and execute unauthorized code.

Exploitability

High: An attacker requires local access to the system to exploit this vulnerability. The vulnerability may also be exploited over the network, but this attack scenario is not available to low-privileged users in default configurations.

CVE Reference

CVE-2022-29594

Technical Details

A Local Privilege Escalation (LPE) vulnerability exists in default installations of eG Agent where a low-privileged user can elevate privileges to the `NT AUTHORITY\SYSTEM` account due to weak file permissions.

Mitigation

This issue was patched in eG Agent version 7.2.

Discovery Credits

Thibault Van Geluwe de Berlaere, Mandiant

Disclosure Timeline

- 26 April 2022 - Issue reported to vendor
- 28 April 2022 - Vendor created patch and asked Mandiant to verify
- 03 May 2022 - Mandiant confirmed patch remediates the vulnerability
- 06 May 2022 - Vendor published patch and notified customers

References

- eG Innovations Advisory (CVE-2022-29594)
- Mitre CVE-2022-29594