MNDT-2022-0001

Check Point Enterprise Endpoint Security Client for Windows contains a local privilege escalation vulnerability prior to version E86.20

Impact

High - Exploiting the vulnerability will give a local unprivileged attacker SYSTEM level privileges.

Exploitability

Medium - Any authenticated local user can exploit the vulnerability and an exploit is trivial to produce.

CVE Reference

CVE-2021-30360

Technical Details

The installation of the agent uses the Windows Installer framework and an MSI file is cached in c:\windows\installer. An unprivileged user can trigger a repair operation, either by using the Windows Installer API or by running "msiexec.exe /fa c:\windows\installer\[XXXXX].msi".

Running a repair operation will trigger a number of file operations in the %TEMP% folder of the user triggering the repair. Some of these operations will be performed from a SYSTEM context (started via the Windows Installer service), including the execution of temporary files.

Resolution

The issue was fixed in version E86.20; update to this version to address the vulnerability.

Discovery Credits

- Ronnie Salomonsen, Mandiant

Disclosure Timeline

- 19-Oct-2021 - Issue reported to Check Point
- 22-Oct-2021 - Issue confirmed by Check Point and a fix scheduled for January 5, 2022.
- 05-Jan-2022 - Patched version released by Check Point

References

- https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk176853
- https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&solutionid=sk142952
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-30360