CVE-2022-0354: Local Privilege Escalation

Lenovo Commercial Vantage Tool

nto the great resource Windows Internals (Windows Internals Part 1 7th Edition) you will uses the mechanism of Mandatory Integrity Control (MIC) based on Integrity Levels to an objects among each other against unauthorized access. In the following table from the you can see a list of the used Integrity Levels under Windows 10.

ty level SIDs

ame (Level)	Use
ntrusted (0)	Used by processes started by the Anonymous group. It blocks most write access.
ow (1)	Used by AppContainer processes (UWP) and Protected Mode Internet Explorer. It blocks write access to most objects (such as files and registry keys) on the system.
edium (2)	Used by normal applications being launched while UAC is enabled.
igh (3)	Used by administrative applications launched through elevation when UAC is enabled, or normal applications if UAC is disabled and the user is an administrator.
ystem (4)	Used by services and other system-level processes (such as Wininit, Winlogon, Smss, and so on).
rotected (5)	Currently unused by default. Can be set by kernel-mode caller only.

an unprivileged user (medium integrity) logs on to Windows, there is an kernel object alled an access token. This token includes your identity and the current privileges of the team perspective this means, also if I was able to compromise an unprivileged user integrity), still I am not allowed to access processes and objects which need to high the the space of the process. A little more precise, in case of processes it is not possible to the address memory of process which manage high integrity threats, from a process

Escalation: Insecure GUI

not allowed as a medium integrity user to directly access the address memory from a high or example by process injection, there are still scenarios which gives you a possibility to egrity process to escalate your local privileges. For example, in my case by finding the 022-0354 or LEN-76673 in context of the Lenovo Commercial Vantage Tool and how the ntel Management Engine software update packages (and other packages). At New Year's gged in to my Lenovo (as usual as unprivileged user (medium integrity)) and started the l Vantage tool in the same context (medium integrity). I got the suggestion for the **Intel ate Intel Management Engine Firmware 11.8.90.3987** and started the installation. el ME update was initialized immediately, but compared to other updates that I have enovo Commercial Vantag tool, it seemed strange to me that a Windows command shell ing the update. It was not possible to execute directly a command via command line, but I xamined via process explorer with which integrity level the opened update window is ected and hoped (from research perspective to get my first CVE 😅), the **corresponding** as executed in **system integrity level**. Despite the fact, that no direct command can be mmand prompt window, there is still a way (insecure GUI) to use the privileged process tegrity) to escalate from an unprivileged user (medium integrity) to system privileges. We command prompt window context menu from the privileged cmd.exe process to escalate rity level to system integrity. In case of CVE-2022-0354, have a look at the video below.

with Lenovo, the **flaw is in the legacy packaging process for system udpates**. To resolve enovo PSRIT fixed the packaging process for packages which are released after 2022-02- I am not really sure, if Lenovo did fix also the affected legacy packages or only fixed it for re released after 2022-02-25. The **last test** where I was able to escalate to system **e at 2022-04-10** with the **Intel Thunderbold Driver-10 [64]** update package (video below). Thunderbold Driver-10 [64] package was identified just a few days ago, with beginning of t, the following packages are known and affected, and let escalate your unprivileged user to system privileges (System Integrity).

e update Intel Management Engine Firmware 11.8.90.3987 (Found by Infosec Tirol)
Driver – 10 [64] – 17.4.80.550 (Found by Infosec Tirol)

nit für Sicherheit in der Informationstechnik has published a technical safety note with risk level (risk level 4).

to thank Lenovo and the responsible employee Blake for the good cooperation. More he vulnerability on the **Lenovo Website**.

ps://nvd.nist.gov/vuln/detail/CVE-2022-0354

ps://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/TW/2022/04/warnmeldung_tw-t22-0089.html

ps://vuldb.com/de/?id.198433

ps://debricked.com/en/vulnerability-database/vulnerability/CVE-2022-0354

ps://www.heise.de/news/Lenovo-System-Update-koennte-Schadcode-auf-Computer-lassen-6740544.html

ndows internals. Part 1 Seventh edition; Yosifovich, Pavel; Ionescu, Alex; Solomon, David A.; Russinovich, Mark E.

Daniel Feichter

View all posts by Daniel Feichter →

5

Article Rating

Abonnieren

Hinterlassen Sie den ersten Kommentar!

0 COMMENTS