3 important reasons why you should keep your drivers up to date

CapaServices

If a hacker gets access to your operating system's kernel through a driver and disables both the antivirus and the firewall, what good will it do if the software is updated?

Introduction

Many of us do not realise how important it is to keep our computers' drivers and firmware up to date. The Windows and antivirus and firewall products we do update, but drivers and firmware are something we tend to overlook.

There are several reasons why it is important to keep your drivers and firmware up to date:

- Critical security holes are plugged
- Computers operates more stably
- Computers have better performance

In particular, the release cycle for Windows 10 used by Microsoft requires frequent updating of drivers and firmware for the system to have stable operation. Drivers and firmware namely often follow with the Windows version.

Security

At the annual DEFCON hacking conference, which was held in August 2019, the security firm Eclypsium presented the results of a study that documented security holes in more than 40 drivers from at least 20 different providers.

One look at the websites of the major computer manufacturers reveals that they release a good many driver updates that are aimed at plugging security holes monthly.

The largest manufacturers have released more than 30 updates for drivers suffering from critical security holes in the spring of 2020 alone.

Most security holes are plugged shortly after being discovered. Among other things, it took the manufacturers only a couple days after Eclypsium documented the security holes to release updated drivers. This demonstrates, in no uncertain terms, that manufacturers are also aware of the importance of prioritising security in connection with drivers.

There has been an uptick in ransomware attacks of more than 300% from 2018 to 2019!

Even if most ransomware attacks do not directly target driver vulnerabilities, this shows that the need for keeping drivers and firmware up to date has not diminished — quite the reverse.

For example, in 2019, the local government in Baltimore was infected by the ransomware RobbinHood, which takes advantage of a critical driver vulnerability. The attack affected more than 10,000 computers at an overall cost of DKK 120 million.

CapaSystems
...because time matters

CapaSystems A/S
Roskildevej 342C
DK-2630 Taastrup

(+45) 70 10 70 55
sales@capasystems.com

RobbinHood exploits a critical vulnerability in a kernel driver from Gigabyte — even though the driver is approved and digitally signed by the motherboard manufacturer.

((TechAlert))

The vulnerability gives the hacker unlimited access to the entire operating system. Once the ransomware shuts down the computer's security, e.g. antivirus and firewall software, the user-related files on the computer are encrypted, and the user is denied access to them.

Access to the files is only restored if the user pays "ransom".

Functionality

Many IT departments have experienced challenges with the combination of Thunderbolt docks and one or more external monitors. The solution in the vast majority of cases has been to upgrade the firmware and drivers.

Likewise, many IT departments have had challenges with the fan in Microsoft Surface, which has run almost constantly. The solution here has also often been to update the firmware and drivers.

Performance & Stability

Drivers and firmware have a significant impact on a computer's performance and stability, but it is difficult to assess their specific effect. The typical impression is only that the computer "is running better".

As a specific example, in the summer of 2019, NVIDIA released their Gamescom Game Ready Driver, which improves the performance of some of their graphics cards by up to 23%.

Solutions

Most companies update their hardware drivers when they install a new computer, but there is rarely a focus on keeping drivers up to date afterwards.

The are some third-party products available on the market that can help keep a computer's drivers up-to-date, but they primarily target the B2C market.

Many major hardware manufacturers have a separate software tool for managing driver updates, but if a company has hardware from several different manufacturers, they can quickly get complicated to administrate.

At CapaSystems, we have developed a unique service that targets the B2B market and uses a technology that is already built into Windows, and we call it **CapaDrivers** !

CapaSystems A/S
Roskildevej 342C
DK-2630 Taastrup
(+45) 70 10 70 55
sales@capasystems.com