Norway parliament data stolen in Microsoft Exchange attack

bleepingcomputer.com/news/security/norway-parliament-data-stolen-in-microsoft-exchange-attack/

Lawrence Abrams

By
Lawrence Abrams

- March 10, 2021
- 10:57 AM
- 0

Norway's parliament, the Storting, has suffered another cyberattack after threat actors stole data using the recently disclosed Microsoft Exchange vulnerabilities.

Last week, Microsoft released emergency security updates for Microsoft Exchange to fix zero-day vulnerabilities, known as ProxyLogon, used in attacks.

These attacks were originally attributed to a China state-sponsored hacking group known as HAFNIUM who used the vulnerabilities to compromise servers, install backdoor web shells, and gain access to internal corporate networks.

Storting hacked through Exchange server

Soon after suffering a cyberattack in December, the Storting today announced a new cyberattack linked to the recent Microsoft Exchange vulnerabilities.

"The Storting has again been hit by an IT attack. The attack is linked to vulnerabilities in Microsoft Exchange, which affected several businesses.

"The Storting does not yet know the full extent of the attack. A number of measures have been implemented in our systems, and the analysis work is ongoing. The Storting has received confirmation that data has been extracted," the Storting disclosed in a statement.

At this time, the Storting has confirmed that the threat actors have stolen data as part of the cyberattack but are still investigating.

"We know that data has been extracted, but we do not yet have a full overview of the situation. We have implemented comprehensive measures and cannot rule out that it will be implemented further."

"The work takes place in collaboration with the security authorities. The situation is currently unclear, and we do not know the full potential for damage," says Storting director Marianne Andreassen.

However, they do not believe this attack is related to their cyberattack in December 2020, attributed to the Russian APT 28 state-sponsored hacking group.

While Microsoft initially attributed the recent Microsoft Exchange server attacks on a Chinese hacking group known as Hafnium, we have later learned that other hacking groups had been using them as well.

According to a new report by cybersecurity firm ESET, in addition to Hafnium, other cybercrime groups known as Tick, LuckyMouse, and Calypso had also been exploiting the zero-day vulnerabilities before the patches were released.

In a new report released today, ESET states that even more hacking groups are jumping into the Microsoft Exchange frenzy as they rush to hack systems before they are patched.

Related Articles:

Cisco urges admins to patch IOS XR zero-day exploited in attacks

Chinese hackers behind most zero-day exploits during 2021

Google Chrome emergency update fixes zero-day used in attacks

Microsoft April 2022 Patch Tuesday fixes 119 flaws, 2 zero-days

New Spring Java framework zero-day allows remote code execution

- Microsoft Exchange
- Norway
- Parliament
- Storting
- Vulnerability
- Zero-Day

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

You may also like: