Threat Image

As we enter August, we're leaving July behind, but not without the unsettling news that hackers had continuous access to Norway's government Mobile Device Management (MDM) platform for months. MDM systems are attractive targets for threat actors because they provide elevated access to thousands of mobile devices. This situation raised concerns for the Norwegian National Security Authority (NSM) and the American Cybersecurity and Infrastructure Security Agency (CISA), as they feared potential widespread exploitation in government and private sector networks. (1)

At the beginning of August, NSM and CISA revealed a joint Cybersecurity Advisory (CSA) titled 'Threat Actors Exploiting Ivanti EPMM Vulnerabilities.' It highlights that Advanced Persistent Threat (APT) actors exploited a zero-day vulnerability from at least April 2023 to July 2023. The vulnerability was utilized to extract information from multiple Norwegian organizations, as well as to infiltrate and compromise a Norwegian government agency's network. (1)

The advisory outlines the vulnerabilities related to the exploitation, and it provides indicators of compromise (IOCs) and tactics, techniques, and procedures (TTPs). It also includes a nuclei template to identify unpatched devices, and detection guidance organizations can use to hunt for compromise. If potential compromise is detected, organizations should apply the incident response recommendations included. If no compromise is detected, organizations should still immediately apply patches released by Ivanti. (1)

In a recent statement, CISA highlights the significance of UEFI as a vulnerable target for attacks. UEFI code, comprising various components like security initializers, bootloaders, and drivers, exposes systems to persistent and stealthy attacks. CISA emphasized that attackers' success depends on the compromised phase and element of UEFI, but persistence is a common factor. The agency referenced the BlackLotus bootkit as an example of vulnerabilities beneath the operating system. While Microsoft has offered guidance for manual mitigation, CISA plans to collaborate on implementing a Secure by Default update distribution with Microsoft. (2)

Threats manifest in diverse forms, and this serves as a reminder to remain vigilant, as appearances can be deceiving. At the beginning of August, numerous Norwegian phone numbers were targeted, with text messages urging Muslims to retaliate for the recent Quran burnings in Sweden and Denmark. These messages were crafted to suggest involvement by Hezbollah leaders. Nevertheless, investigations by the Norwegian Police Security Service (PST) point towards a foreign hacking group being responsible for these messages. The purpose was likely not rooted in religious motivations, but aimed at fostering unrest, division, and destabilization within Norwegian society. (3)

Latest Cyberthreats and Advisories (4)

- Vulnerability Leaves 900,000 MikroTik Routers Open to Attack
- IBM Report Reveals Cost of Data Breach Now Averages a Record $4.45 Million
- New Details in JumpCloud Breach Reveal North Korean Actors behind the Attack
- The Myth of Mac Invincibility to Cyberattacks
- Ransomware Attacks Climb to Disturbing New Heights in June

(1) https://nsm.no/aktuelt/joint-cybersecurity-advisory-fra-nsm-ncsc-og-cisa
(2) https://www.securityweek.com/cisa-calls-urgent-attention-to-uefi-attack-surfaces/
(3) https://www.nrk.no/norge/pst_-hevnmeldinger-etter-koranbrenninger-trolig-sendt-av-hackergruppe-1.16505022
(4) https://blog.isc2.org/