WEEKLY BULLETIN

7-11 AUGUST 2023

Quote of the week

> *"Security is always excessive until it's not enough."*
>
> **Robbie Sinclair**

Content:

- **CISA warns organizations about exploited vulnerabilities affecting .NET, Visual Studio**
- **Intel addresses 80 vulnerabilities affecting its products**
- **UK voter data exposed in Electoral Commission cyber attack**
- **Microsoft - Patching Alert**

CISA warns organizations about exploited vulnerabilities affecting .NET, Visual Studio

The US Cybersecurity and Infrastructure Security Agency (CISA) has added a zero-day flaw affecting Microsoft's .NET and Visual Studio products to the Catalog of Known Vulnerabilities.
The vulnerability, tracked as CVE-2023-38180, was patched by Microsoft with its August 2023 Patch Tuesday updates, which also address CVE-2023-36884, an Office vulnerability exploited by Russian threat actors.

Microsoft reveals that remote exploitation is possible and no user interaction is required.
The CISA catalog also includes several other exploited vulnerabilities affecting .NET and/or Visual Studio.
Read more

Intel addresses 80 vulnerabilities affecting its products

Intel recently issued a total of 46 new security advisories to inform customers about 80 vulnerabilities affecting the company's firmware and software.
The most serious vulnerabilities, based on their CVSS score, are 18 high-severity issues that allow privilege escalation or, in some cases, denial-of-service (DoS) attacks.
These mainly allow a local attacker to escalate privileges, and some can lead to information disclosure or DoS attacks.

Most of these discovered vulnerabilities have received patches, but some of the affected products have been discontinued.
Read more

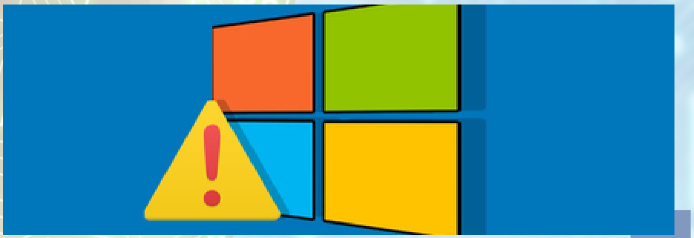
UK voter data exposed in Electoral Commission cyber attack

The United Kingdom's Electoral Commission has revealed that it was the victim of a "sophisticated cyber attack", exposing the personal data of millions of British voters.
Malicious actors accessed "reference copies" of electoral registers maintained by the Commission for research purposes and to enable checks on the permissibility of political donations. This contained the personal details of anyone in the UK who registered to vote between 2014 and 2022, including names and home addresses. The names of those registered as voters abroad were also exposed.

There is currently no indication of who may have been behind the breach.

Read more

PATCHING ALERT



Microsoft releases patches for 74 new vulnerabilities in August update.

Microsoft has patched a total of 74 vulnerabilities in its software as part of the company's August 2023 updates.
This includes six critical, 67 important, and one moderate severity vulnerability. Also released along with the security improvements are two security-in-depth updates for Microsoft Office (ADV230003) and the Memory Integrity System Readiness Tool (ADV230004).
Microsoft announced that installing the latest update "stops the chain of attack" that leads to the remote code execution bug.

Read more