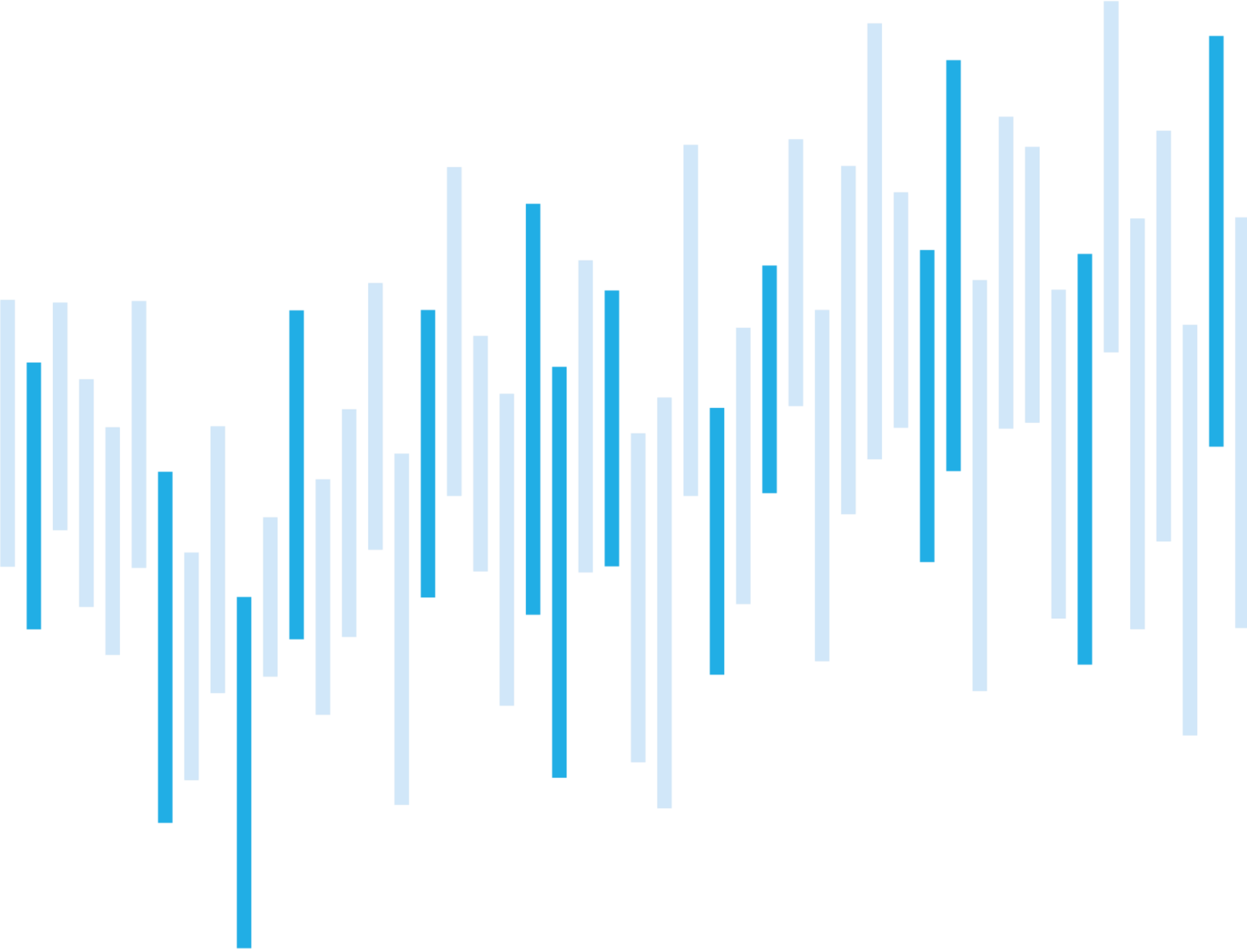
# CYBER SECURITY INCIDENTS FROM THE NÚKIB’ S PERSPECTIVE

## March 2024



National Cyber
and Information
Security Agency

## Summary of the month

The number of incidents recorded in March was identical to the previous month. It was the fifth month in a row with below average figures of registered incidents. As in February, one significant cyber incident was recorded. The remaining 17 incidents fell into the category of less significant.

Availability-related incidents continue to dominate the summary. Incidents from the categories of Penetration and Information Security were also registered and compared to February, Malicious Code, as well.

In the Focus on the Threat chapter, this time we look at the discovery of the compromised XZ tool, which is used by most Unix operating systems. Within a complex and long-running operation, a so far unknown actor planted a backdoor in it in order to gain access to a large number of devices. In response to the incident, a number of warnings were issued, in particular by companies distributing various Linux variants.

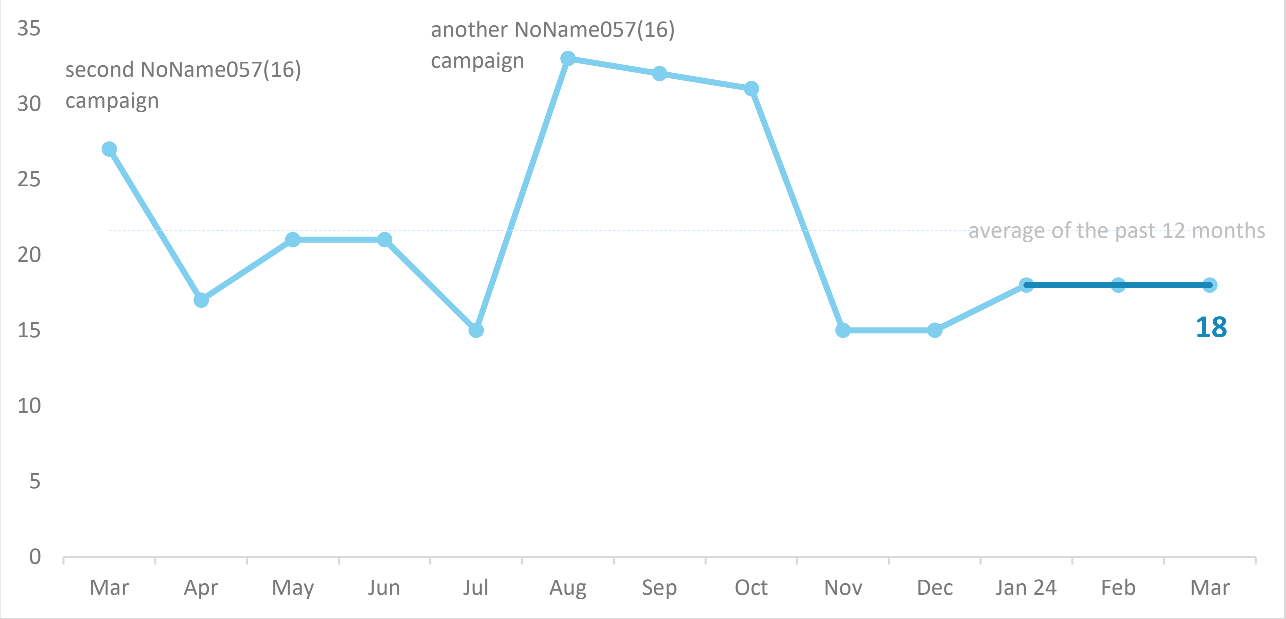
## Table of content

The following report summarises the events of the month. The data, information and conclusions contained herein are primarily based on cyber incidents reported to NÚKIB. If the report contains information from open sources in some sections, the origin of this information is always stated.

You can send comments and suggestions for improving the report to the address komunikace@nukib.cz

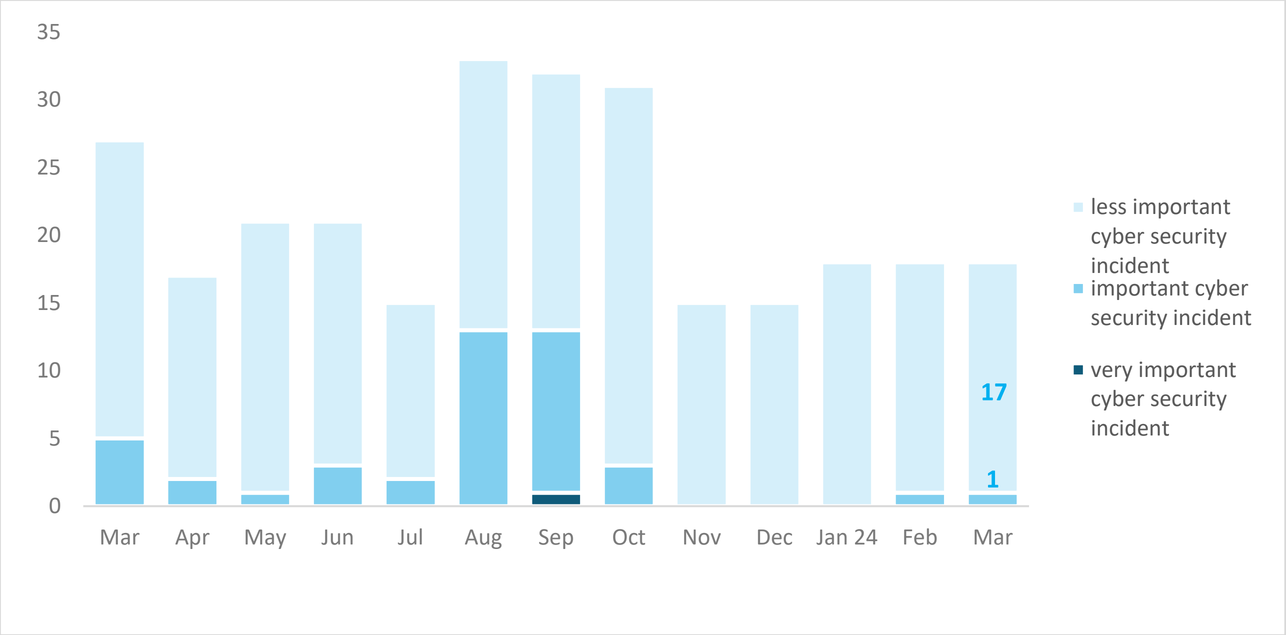
## Number of cyber security incidents reported to NÚKIB[1]

The number of incidents recorded in March was identical to the previous month. It was the fifth month in a row with below average figures of registered incidents.



## Severity of the handled cyber security incidents[2]

As in February, one significant cyber incident was recorded. The remaining 17 incidents fell into the category of less significant.



[1] NÚKIB registered 16 incidents in total with liable entities according to Cyber Security Act. The remaining 2 incidents involved unregulated entities.

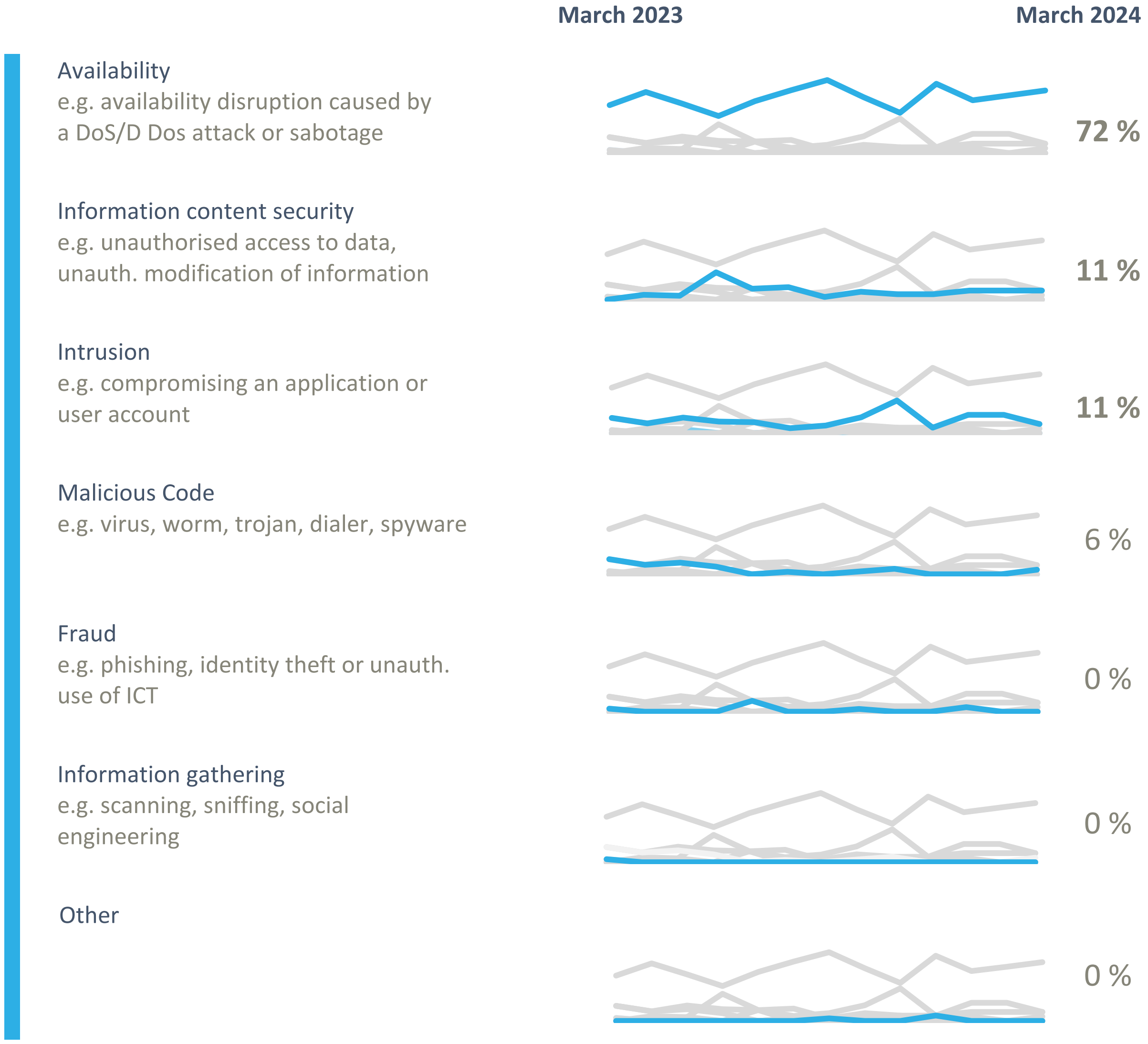
[2] NÚKIB determines the severity of cyber incidents on the basis of Decree No. 82/2018 Coll. and its internal methodology.

## Classification of the incidents reported to NÚKIB [3]

The long-term dominance of availability-related incidents persisted also in March while this category consisted exclusively of DDoS attacks.

NÚKIB further solved incidents in these three categories:

- Two incidents, both of which were ransomware attacks, fell into the Information security category. One of the attacks was perpetrated by the LockBit 3.0 group, while NÚKIB has no information about the attacker in the second incident.
- NÚKIB recorded two incidents within the Intrusion category involving compromised user accounts. However, these compromises did not result in any data leakage, nor did they lead to further impacts.
- The final category involved Malicious Code, specifically the exploitation of vulnerabilities in Ivanti products. This exploitation resulted in the compromise of VPNs and the subsequent exfiltration of data.



[3] The cyber incident classification is based on the ENISA taxonomy: Reference Incident Classification Taxonomy — ENISA (europa.eu)

## March trends in cyber security from the NÚKIB's perspective [4]

### ❯ Phishing, spear-phishing and social engineering

In March, NÚKIB registered only two incidents in which the use of phishing was confirmed. The attackers managed to provoke the victim into filling in login details on a fraudulent site and then misuse these details to access other services.

### Malware ❯

Similar to previous months, continuous malware analysis activities were also conducted in March in connection with previously registered incidents.

### ❯ Vulnerabilities

NÚKIB did not issue any alerts regarding vulnerabilities in March. However, one incident exploited a legacy vulnerability in Ivanti products to compromise VPNs and other malicious activities. In addition, the backdoor in the XZ tool was designated as CVE-2024-3094 with the highest severity rating of 10.

### Ransomware ↗

Two ransomware-related incidents were recorded in March. LockBit 3.0 group is responsible for one of them, for the second incident, NÚKIB does not have information about the perpetrators of the attack.

### ↗ Attacks on availability

Throughout March, NÚKIB recorded more than ten DDoS attacks, primarily targeting state institutions. A Russian-speaking hacktivist group was behind three of the incidents, while the attacker remains unknown for the rest.

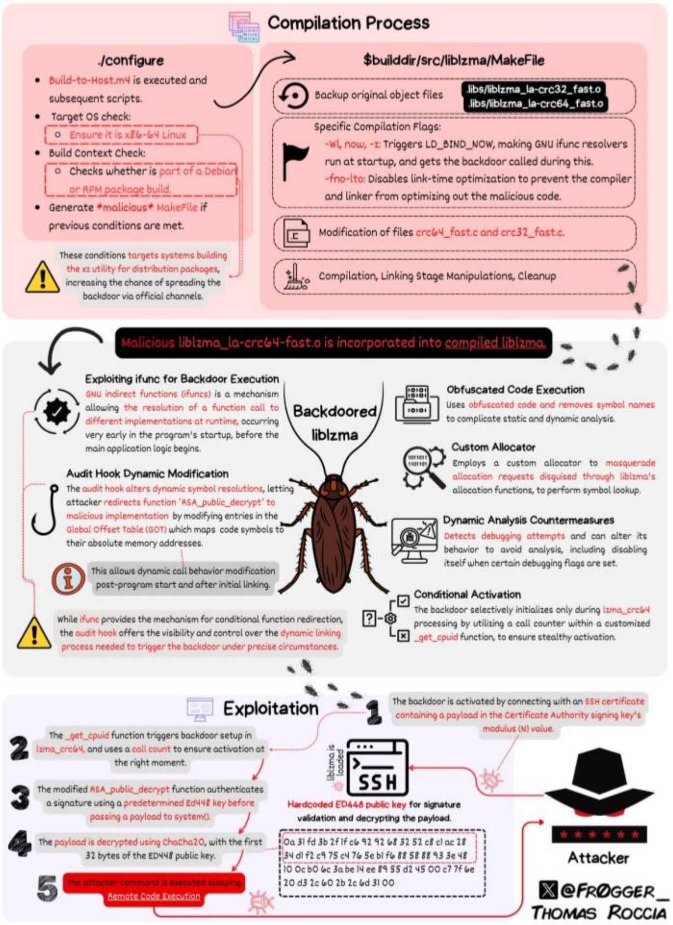
[4] The development illustrated by the arrow is evaluated in relation to the previous month.

## Focus on a threat: Compromise of the XZ tool on Unix-based systems

A Microsoft developer detected that the Linux tool XZ (an open-source data compression tool) contained a deliberately embedded backdoor on Friday 29th March. It is assumed that the attackers had been working on the compromise for years, and the backdoor was supposed to have made its way into Debian and Fedora products, some of the largest Linux distributions. Given the complex nature of the campaign, this is one of the best executed supply chain attacks.

XZ provides a lossless data compression on virtually all Unix-like operating systems, including Linux. **The vulnerability is identified as CVE-2024-3094, with a critical and maximum value of 10 on the CVSS scale.** Despite the complexity of the operation, the attack was detected in time, as it did not penetrate stable systems, but only test versions. Malicious code if executed, could have enabled the eventual takeover of the victim's device.

Fig. 1: Diagram of the compromised XZ library function (higher resolution)



- Build-to-Host.m4 is executed and subsequent scripts.
- Target OS check:
  - Ensure it is x86-64 Linux
- Build Context Check:
  - Checks whether is part of a Debian or RPM package build.
- Generate *malicious* MakeFile if previous conditions are met.

These conditions targets systems building the xz utility for distribution packages, increasing the chance of spreading the backdoor via official channels.

Backup original object files .libs/liblzma_la-crc32_fast.o .libs/liblzma_la-crc64_fast.o

Specific Compilation Flags:
-Wl, now, -z: Triggers LD_BIND_NOW, making GNU ifunc resolvers run at startup, and gets the backdoor called during this.
-fno-lto: Disables link-time optimization to prevent the compiler and linker from optimizing out the malicious code.

Modification of files crc64_fast.c and crc32_fast.c.

Compilation, Linking Stage Manipulations, Cleanup

Malicious liblzma_la-crc64-fast.o is incorporated into compiled liblzma.

Exploiting ifunc for Backdoor Execution
GNU indirect functions (ifuncs) is a mechanism allowing the resolution of a function call to different implementations at runtime, occurring very early in the program's startup, before the main application logic begins.

Audit Hook Dynamic Modification
The audit hook alters dynamic symbol resolutions, letting attacker redirects function 'RSA_public_decrypt' to malicious implementation by modifying entries in the Global Offset Table (GOT) which maps code symbols to their absolute memory addresses.

This allows dynamic call behavior modification post-program start and after initial linking.

While ifunc provides the mechanism for conditional function redirection, the audit hook offers the visibility and control over the dynamic linking process needed to trigger the backdoor under precise circumstances.

Obfuscated Code Execution
Uses obfuscated code and removes symbol names to complicate static and dynamic analysis.

Custom Allocator
Employs a custom allocator to masquerade allocation requests disguised through liblzma's allocation functions, to perform symbol lookup.

Dynamic Analysis Countermeasures
Detects debugging attempts and can alter its behavior to avoid analysis, including disabling itself when certain debugging flags are set.

Conditional Activation
The backdoor selectively initializes only during lzma_crc64 processing by utilizing a call counter within a customized _get_cpuid function, to ensure stealthy activation.

1 The backdoor is activated by connecting with an SSH certificate containing a payload in the Certificate Authority signing key's modulus (N) value.

2 The _get_cpuid function triggers backdoor setup in lzma_crc64, and uses a call count to ensure activation at the right moment.

3 The modified RSA_public_decrypt function authenticates a signature using a predetermined Ed448 key before passing a payload to system().

4 The payload is decrypted using ChaCha20, with the first 32 bytes of the ED448 public key.

5 The attacker command is executed allowing Remote Code Execution

Hardcoded ED448 public key for signature validation and decrypting the payload.

```
0a 31 fd 3b 2f 1f c6 92 92 68 32 52 c8 c1 ac 28
34 d1 f2 c9 75 c4 76 5e b1 f6 88 58 88 93 3e 48
10 0c b0 6c 3a be 14 ee 89 55 d2 45 00 c7 7f 6e
20 d3 2c 60 2b 2c 6d 31 00
```

Source: x.com

In response to the incident, a number of companies, including Microsoft and Red Hat, issued warnings and recommendations to downgrade operating systems to the last known secure version. Similar alert was also issued by the U.S. Cyber and Infrastructure Security Agency (CISA)

## Probability terms used

Probability terms and expressions of their percentage values:

| Term | Probability |
|---|---|
| Almost certain | 90–100 % |
| Highly likely | 75–85 % |
| Likely | 55–70 % |
| Realistic probability | 25–50 % |
| Unlikely | 15–20 % |
| Highly unlikely | 0–10 % |

## Traffic Light Protocol

The information provided shall be used in accordance with the Traffic Light Protocol methodology (available at the website https://ww.first.org/tlp/). The information is marked with a flag, which sets out conditions for the use of the information. The following flags are specified that indicate the nature of the information and the conditions for its use:

| Colour | Conditions of use |
|---|---|
| TLP:RED | For the eyes and ears of individual recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. |
| TLP:AMBER+STRICT | Restricts sharing to the organization only. |
| TLP:AMBER | Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. |
| TLP:GREEN | Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defence community. |
| TLP:CLEAR | Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction. |