Scottish Cyber Coordination Centre

# Daily threat bulletin

5 April 2024

## Vulnerabilities

### Microsoft fixes Outlook security alerts bug caused by December updates

BleepingComputer - 04 April 2024 16:14

Microsoft has fixed an issue that triggers erroneous Outlook security alerts when opening .ICS calendar files after installing the December 2023 Outlook Desktop security updates [...]

### HTTP/2 CONTINUATION Flood technique can be exploited in DoS attacks

Security Affairs - 05 April 2024 03:41

HTTP/2 CONTINUATION Flood: Researchers warn of a new HTTP/2 vulnerability that can be exploited to conduct powerful denial-of-service (DoS) attacks. HTTP messages can contain named fields in both header and trailer sections. CERT/CC experts explained that both header and trailer fields are serialized as field blocks in HTTP/2 to transmit them in multiple fragments to [...]

### Critical Vulnerability in Progress Flowmon Allows Remote Access to Systems

SecurityWeek - 04 April 2024 13:23

A critical OS command injection in Progress Flowmon can be exploited to gain remote, unauthenticated access to the system.The post Critical Vulnerability in Progress Flowmon Allows Remote Access to Systems appeared first on SecurityWeek.

## Threat actors and malware

### New Latrodectus malware replaces IcedID in network breaches

BleepingComputer - 04 April 2024 17:38

A relatively new malware called Latrodectus is believed to be an evolution of the IcedID loader, seen in malicious email campaigns since November 2023. [...]

### Visa warns of new JSOutProx malware variant targeting financial orgs

BleepingComputer - 04 April 2024 16:29

Scottish Cyber Coordination Centre

Visa is warning about a spike in detections for a new version of the JsOutProx malware targeting financial institutions and their customers. [...]

## Vietnam-Based Hackers Steal Financial Data Across Asia with Malware

The Hacker News - 04 April 2024 22:12

A suspected Vietnamese-origin threat actor has been observed targeting victims in several Asian and Southeast Asian countries with malware designed to harvest valuable data since at least May 2023.Cisco Talos is tracking the cluster under the name CoralRaider, describing it as financially motivated. Targets of the campaign include India, China, South Korea, Bangladesh, Pakistan, Indonesia,

## New Phishing Campaign Targets Oil & Gas with Evolved Data-Stealing Malware

The Hacker News - 04 April 2024 22:00

An updated version of an information-stealing malware called Rhadamanthys is being used in phishing campaigns targeting the oil and gas sector."The phishing emails use a unique vehicle incident lure and, in later stages of the infection chain, spoof the Federal Bureau of Transportation in a PDF that mentions a significant fine for the incident," Cofense researcher Dylan Duncan said.The

## Leicester Council Confirms Confidential Documents Leaked in Ransomware Attack

Infosecurity Magazine - 04 April 2024 13:00

Leicester City Council confirmed around 25 sensitive documents have been leaked online, including personal ID information, following claims by the Inc Ransom gang

## Threat Actor Claims Classified Five Eyes Data Theft

Infosecurity Magazine - 04 April 2024 10:30

Threat actor IntelBroker claims to have classified intelligence stolen from US government tech supplier Acuity