Newsletter

Friday, September 20, 2024

TOP NEWS

Cyber criminals Exploit HTTP Headers for Credential Theft via Large-Scale Phishing Attacks

High-profile data breaches affecting large organizations

HACKERS EXPLOIT DEFAULT CREDENTIALS IN FOUNDATION SOFTWARE TO BREACH CONSTRUCTION FIRMS

Threat actors have been observed targeting the construction sector by infiltrating the FOUNDATION Accounting Software. A consequence of this action is that threat actors could brute force the server to run arbitrary shell commands. To mitigate the risk posed it's recommended to rotate default account credentials and cease exposing the application over the public internet if possible.

New System Update

Phishing and Social Engineering

Phishing remains a prevalent method for cybercriminals to gain access to sensitive information. Recent campaigns have targeted businesses and individuals, often using sophisticated tactics. Always verify the sender's email address, avoid clicking on suspicious links, and report any suspicious emails to your IT department.

BEWARE: PHISHING SCAMS EVERYWHERE!

Threat Actor Allegedly Claim Breach of Dell Employee Data

A hacking forum post has raised concerns over a potential Dell Technologies data breach. The breach allegedly affects 10,800 employees and partners and exposes sensitive internal data. The leaked information includes employee IDs, full names, employment status, and internal identification numbers.

The company stated that its security team is actively examining the allegations to determine their validity and assess any potential impact.At this time, Dell has not confirmed whether the breach was due to external hacking or an internal security lapse.

Data breaches pose significant risks to organizations, often leading to financial losses, reputational damage, and legal consequences.

INTRODUCING NEW COURSE!!

RANSOMWARE

Ransomware is malicious software that blocks access to a system or data until a ransom is paid. It encrypts critical files, demanding payment for their release, causing financial losses and operational disruptions. Effective cyber security measures are essential to protect against such attacks.