CYBER WEEKLY 44-2022

‹Trending Cybersecurity news updates ›

MONDAY (7th November)

Medibank Confirms Data Breach Impacts 9.7 Million Customers

Australian health insurer Medibank today confirmed that the data of 9.7 million customers was compromised in a recent cyberattack.

The incident was identified on October 12, before threat actors could deploy file-encrypting ransomware, but not before they stole data from the company's systems. Medibank, which immediately initiated incident response and launched an investigation into the attack, could not determine whether customer data was compromised until contacted by the threat actor behind the data breach.

Health claims data for some Medibank, ahm, and international customers was also compromised, including service provider's name and location, the location where medical services were provided, and diagnosis and procedures codes.

Two weeks ago, the company estimated that roughly 4 million customers might have been impacted by the cyberattack, but it has now increased that estimate to 9.7 million.

Medibank announced that it now believes the attackers exfiltrated all of the customer data they were able to access during the incident, but said that it will not pay any ransom demand.

The company, which has restored services impacted by the incident and has maintained business operations during the event, says that no further suspicious activity has been identified inside its network since October 12.

TUESDAY (8th November)

Canadian Meat Giant Maple Leaf Foods Disrupted by Cyberattack

Canadian meat giant Maple Leaf Foods has confirmed that it is experiencing an outage after falling victim to a cyberattack. Created in 1991 by the merger of Canada Packers and Maple Leaf Mills, the packaged meats company is headquartered in Mississauga, Ontario.

Maple Leaf Foods has more than 14,000 employees and has market presence in Canada, the US, and Asia, offering products under several brands, including Maple Leaf, Schneiders, Mina, Greenfield Natural Meat Co., Lightlife, and Field Roast.

Over the weekend, the company fell victim to a cyberattack that resulted in system disruptions, the company has announced, without sharing further details on the incident.

Maple Leaf Foods said it has executed business continuity plans and that work is underway to restore the impacted systems. However, the company expects further operational and service disruptions, saying that restoration efforts take time.

Maple Leaf is not the first large meat company to have its operations be impacted by a cyberattack. In mid-2021, JBS, the largest meat processing company in the word, was disrupted by a ransomware attack that forced an operational shutdown, just weeks after a similar incident shut down the Colonial Pipeline.

WEDNESDAY (9th November)

Twitter Security Chief Resigns as Musk Sparks 'Deep Concern'

A top security officer for Twitter resigned on Thursday as new owner Elon Musk's revamp of the platform saw a boomlet of fake accounts, drawing a rare warning from US regulators.

The walk-outs came a day after the chaotic launch of new features introduced by Musk following his $44 billion buyout of the influential one-to-many messaging app.

It unveiled its long-awaited Twitter Blue subscription service, which allows users to pay $7.99 per month for a coveted blue tick, as well as a separate gray "official" badge for some high-profile accounts. But Musk drew criticism when he scrapped the new gray label almost immediately, overshadowing the launch of the pay service, which is currently only available on the mobile app on iPhones and in the United States.

The chaos drew a rare warning from the Federal Trade Commission, the US authority that oversees consumer safety which has put Twitter under watch for past security and privacy breaches.

He also announced that he was ending work- from-home policies at Twitter, which had been a widespread practice at the San Francisco-based company.

THURSDAY (10th November)

ABB Oil and Gas Flow Computer Hack Can Prevent Utilities From Billing Customers

Oil and gas flow computers and remote controllers made by Swiss industrial technology firm ABB are affected by a serious vulnerability that could allow hackers to cause disruptions and prevent utilities from billing their customers, according to industrial cybersecurity firm Claroty.

Utilities rely on flow computers to calculate oil and gas flow rates and volume. These devices, which are often used in the electric power sector, play an important role in process safety, as well as billing.

Claroty reported its findings to ABB, which announced the release of firmware patches for affected products in July. The path traversal vulnerability is tracked as CVE-2022-0902 and it has been assigned a 'high severity' rating.

ABB has determined that its XFC G5 and uFLO G5 flow computers, RMC-100, XRC G5, and XIO remote controllers, as well as the Totalflow Universal Data Controller (UDC) are impacted. The vendor said in its July advisory that it was not aware of any attacks exploiting the vulnerability. Claroty has published a blog post detailing its research, as well as a video showing how an attacker could hack a device..

FRIDAY (11th November)

Microsoft Blames Russian Hackers for Prestige Ransomware Attacks on Ukraine and Poland

Microsoft on Thursday attributed the recent spate of ransomware incidents targeting transportation and logistics sectors in Ukraine and Poland to a threat cluster that shares overlaps with the Russian state-sponsored Sandworm group. The attacks, which were disclosed by the tech giant last month, involved a strain of previously undocumented malware called Prestige and is said to have taken place within an hour of each other across all victims.

The Microsoft Threat Intelligence Center (MSTIC) is now tracking the threat actor under its element-themed moniker Iridium (née DEV-0960), a Russia-based group that's tracked by the name Sandworm (aka Iron Viking, TeleBots, and Voodoo Bear).

The company also further assessed the group to have orchestrated compromise activity targeting many of the Prestige victims as far back as March 2022, before culminating in the deployment of the ransomware on October 11.

Microsoft, in its Digital Defense Report published last week, further called out Iridium for its pattern of targeting critical infrastructure and operational technology entities.

SATURDAY (12th November)

LiteSpeed Vulnerabilities Can Lead to Complete Web Server Takeover

LiteSpeed Web Server vulnerabilities discovered by researchers at Palo Alto Networks can be exploited to take complete control of a targeted server.

The security holes were discovered during an audit of OpenLiteSpeed, the open-source version of the LiteSpeed performance-focused web server made by LiteSpeed Technologies. Both versions are impacted by the vulnerabilities and they have been patched with the release of OpenLiteSpeed 1.7.16.1 and LiteSpeed 6.0.12.

LiteSpeed is a popular web server and an analysis by Palo Alto Networks showed that it has a 2% market share — others say that it has a much bigger market share — and that it is used by 1.9 million internet-facing instances.

The first vulnerability, rated 'high severity' and tracked as CVE-2022-0073, is related to a field that allows users to specify a command to be executed when the server starts.

The second vulnerability, also rated 'high severity' and tracked as CVE-2022-0074, can be leveraged by an attacker who has exploited the previous flaw to escalate privileges from 'nobody' to 'root'.

The third issue, CVE-2022-0072, is a directory traversal bug that can be exploited to bypass security measures and access forbidden files.

SUNDAY (13th November)

Foxit Patches Several Code Execution Vulnerabilities in PDF Reader

Popular PDF document reader Foxit Reader has been updated to address multiple use-after-free security bugs that could be exploited for arbitrary code execution.

The feature-rich PDF reader provides broad functionality to users, including support for multimedia documents and dynamic forms via JavaScript support, which also expands the application's attack surface.

This week, Cisco's Talos security researchers have published information on four vulnerabilities in Foxit Reader's JavaScript engine that could be exploited to achieve arbitrary code execution.

The issues, tracked as CVE-2022-32774, CVE-2022-38097, CVE-2022-37332 and CVE-2022-40129, have a CVSS score of 8.8 and are described as use-after-free vulnerabilities.

An attacker looking to exploit these vulnerabilities would need to trick a user into opening a malicious file. According to Cisco, if the Foxit browser plugin extension is enabled, the bugs can be triggered when the user navigates to a malicious website.

Cisco reported the security defects to Foxit in September. This week, Foxit released version 12.0.1.12430 of its PDF reader to address all issues. Users are advised to update to the latest software iteration as soon as possible.