DAILY CYBER HEADLINES

Health-ISAC Daily Cyber Headlines

TLP:GREEN

Jun 23, 2021

Today's Headlines:

Leading Story

- SEC Probes SolarWinds Breach Disclosure Failures

Data Breaches & Data Leaks

- Georgia Fertility Clinic Faces Ransomware Attack, SSNs and Medical Info Leaked

Cyber Crimes & Incidents

- US Seizes Iranian and Iranian Proxy Propaganda Domains

Vulnerabilities & Exploits

- SonicWall Bug That Affected 800K Firewalls Was Only Partially Fixed
- Zephyr RTOS Fixes Bluetooth Bugs That May Lead to Code Execution

Trends & Reports

- UK Parliamentary Staffers Lost 96 Devices in Past Two Years
- Ransomware Payments Could Be Tax Deductible; Report

Privacy, Legal & Regulatory

- Nothing to Report

Upcoming Health-ISAC Events

- Health-ISAC Monthly Threat Brief – June 29, 2021 12:00 PM Eastern

Leading Story

SEC Probes SolarWinds Breach Disclosure Failures

Summary

- The United States Securities and Exchange Commission (SEC) has launched a probe to determine whether some companies failed to disclose that they had been impacted by the 2020 hacking attack that compromised the SolarWinds Orion software supply chain.

Analysis & Action

The assault on SolarWinds was discovered and disclosed by researchers at FireEye in December. The advanced persistent threat (APT) group behind the attack was able to compromise nine government agencies, critical infrastructure, and hundreds of private-sector organizations. Last month, SolarWinds CEO Sudhakar Ramakrishna revealed that the attackers may have accessed the

company's system as early as January 2019. The company has said that as many as 18,000 of its customers were affected by the breach.

Two people familiar with the SEC investigation told the news source Reuters that letters were sent out last week by the SEC to a number of investment firms and public issuers. In the missives, the Commission asked the entities to voluntarily state whether they had been victimized by the unprecedented SolarWinds hack and kept quiet about it. The anonymous sources also said that in addition to probing data breach disclosure failures, the SEC is seeking to determine whether the cybersecurity policies at certain companies were designed to protect customer data.

Under United States securities law, companies are required to disclose material information that could affect their share prices, including data on breaches caused by cybersecurity incidents. If the entities that receive the SEC's letters reply by disclosing information about the breaches, they will avoid any enforcement actions linked to internal accounting control failures and historical failures, the sources said.

Data Breaches & Data Leaks

Georgia Fertility Clinic Faces Ransomware Attack, SSNs and Medical Info Leaked

Summary

- Georgia fertility clinic Reproductive Biology Associates, along with affiliate My Egg Bank North America, disclosed that approximately 38,000 patients were impacted by a ransomware attack in April.

Analysis & Action

In a notice from its general counsel, Reproductive Biology Associates and My Egg Bank North stated that they first became aware of a potential data incident on April 16, 2021 they discovered that a file server containing embryology data was encrypted and therefore inaccessible.

After determining that the breach was the result of ransomware, the server was shut down on the same day. The notice said that the actor

gained access to the system on April 7th, 2021, and again on April 10th.

By June 7th, the organization pinpointed the individuals who were impacted and regained access to encrypted files. In addition, it received confirmation from the actor that all data has been deleted. The investigation is still ongoing, but legal counsel said in the notice that lab results, full names, addresses, Social Security numbers, and human tissue information may have been exposed.

As a result of this incident, we have initiated an investigation through a leading professional IT services firm to conduct interviews and analyze forensic data related to the incident, the firm stated. In addition, the clinic has conducted cybersecurity training with staff and added internal controls to prevent future attacks.

Cyber Crimes & Incidents

US Seizes Iranian and Iranian Proxy Propaganda Domains

Summary

- Notices have appeared on a number of Iran-affiliated websites saying they had been seized by the United States government as part of law enforcement action.

Analysis & Action

Iranian news agencies said that the US government had seized several Iranian media websites and sites belonging to groups affiliated with Iran such as Yemen's Houthi movement.

The domain almasirah[.]net has been seized by the United States Government in accordance with a seizure warrant as part of a law enforcement action by the Bureau of Industry and Security, Office of Export Enforcement and Federal Bureau of Investigation, the Masirah TV website reads.

A US Justice Department spokesperson had no immediate comment. Two US government sources indicated that the Justice Department was preparing an announcement on this issue. Notices have also appeared on websites of Iran's Press TV and Lualua TV, a Bahraini independent channel which broadcasts from the UK.

Vulnerabilities & Exploits

SonicWall Bug That Affected 800K Firewalls Was Only Partially Fixed

Summary

- New findings have emerged that shed light on a critical SonicWall vulnerability disclosed last year, which was initially thought to have been patched.

Analysis & Action

In October last year, a critical stack-based Buffer Overflow vulnerability, tracked as CVE-2020-5135, was discovered affecting over 800,000 SonicWall VPNs. When exploited, the vulnerability allows unauthenticated remote attackers to execute arbitrary code on the impacted devices, or cause Denial of Service (DoS). Turns out, the vulnerability was not properly patched; until now.

After a series of emails between Tripwire researcher Young and SonicWall, the vulnerability was eventually treated as a problem and patched. But later on, the researcher retested his proof-of-concept (PoC) exploit against SonicWall instances and concluded that the fix was botched.

The Tripwire researcher was surprised to notice his PoC exploit didn't trigger a system crash but a flood of binary data in the HTTP response instead. This is when Young reached out to SonicWall again for a remedy. Young states that the binary data returned in the HTTP responses could be memory addresses.

As such a new vulnerability identifier, CVE-2021-20019 has been assigned to the flaw. SonicWall is active in collaborating with third-party researchers, security vendors and forensic analysis firms to ensure its products meet or exceed expected security standards, SonicWall stated. SonicWall has now released an advisory related to this vulnerability, with further information on the fixed versions.

The new SonicWall advisory can be accessed here.

Zephyr RTOS Fixes Bluetooth Bugs That May Lead to Code Execution

Summary

- The Zephyr real-time operating system (RTOS) for embedded devices received an update earlier this month that fixes multiple vulnerabilities that can cause a denial-of-service (DoS) condition and potentially lead to remote code execution.

Analysis & Action

The issues were discovered in Zephyr's Bluetooth LE Link Layer (LL) and its implementation of the Logical Link Control and Adaptation Protocol (L2CAP). Despite being a small open-source project, Zephyr is backed by big frims in the industry like Facebook, Google, Intel, Nordic Semiconductors, and Adafruit.

The operating system supports more than 200 boards with various CPU architectures, making it an attractive choice for makers of small, embedded devices, like hearing aids, smart tags, distancing trackers, safety pods for smart PPE, IoT gateways, portable backup devices.

Asenior software engineer at Synopsys, an American electronic design automation (EDA) company, found eight vulnerabilities in Zephyr after testing the lowest layers of the operating system's Bluetooth LE stack. The flaws are all in the Bluetooth LE Link Layer and the L2CAP implementation. Most of them affect Zephyr versions 2.5.0 and 2.4.0; some are also present in version 1.14. Exploiting most of them prevents the vulnerable device from working either by causing them to freeze or misbehave in a way that prevents other systems from connecting to it.

A new Zephyr version, 2.6.0 has been released at the beginning of the month to include fixes for all the security vulnerabilities listed in the Synopsys' report. The full Synopsys report can be accessed here.

Trends & Reports

UK Parliamentary Staffers Lost 96 Devices in Past Two Years

Summary

- Close to 100 electronic devices have been lost by Parliamentary staffers in the UK during the last two years, raising fears that sensitive public data has fallen into the hands of malicious actors.

Analysis & Action

The official data obtained by Parliament Street think tank under Freedom of Information (FOI) legislation revealed that a total of 96 laptops, tablet computers and other electronic gadgets were reported missing by Parliamentary staffers in the calendar years of 2019 and 2020.

The majority of the device loss incidents occurred in 2019, at 53, with the remaining 43 taking place in 2020. Of the 96 lost or stolen devices, 41 were laptops, 36 were tablets, and the reminder included 11 phones and six skype headsets.

Of the 76 devices reported as lost, 11 were on trains, three on a bus, six in a car and even one in a pub. Of the 20 devices that were stolen, four were from home addresses, one in a hotel and one on the London Underground. Worryingly, just 18 of the total number of devices reported missing were subsequently located and found.

If a lost laptop ends up in the wrong hands, the organization in question could be facing a far more costly predicament than first anticipated, stated a vice-president from Absolute Software.

Ransomware Payments Could Be Tax Deductible; Report

Summary

- US organizations that choose to pay a ransom to their online extorters may be eligible to claim the money back from the Internal Revenue Service (IRS), it has emerged.

Analysis & Action

The IRS offers no formal guidance on ransomware payments, but multiple tax experts interviewed by The Associated Press said deductions are usually allowed under law and established guidance. It's a silver lining to ransomware victims, as some tax lawyers and accountants put it. It's unclear how many companies that pay ransomware payments avail themselves of the tax deductions.

But there are limits to the deduction. If the loss to the company is covered by cyber insurance, something that also is becoming more common, the company can't take a deduction for the payment that's made by the insurer, according to tax experts.

An incident response expert at Obrela Security Industries, argued that this IRS oversight will not last long, and probably would eventually be enforced.

Privacy, Legal & Regulatory

Nothing to Report.

Health-ISAC Cyber Threat Level

On June 3, 2021, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively chose to maintain the Threat Level at Blue (GUARDED). TIC members noted current threats facing the healthcare sector with an emphasis on recent events involving ongoing ransomware attacks, increased observances of Qbot malware, an uptick in phishing campaigns, and unemployment insurance fraud.

For more information about the Health-ISAC Cyber Threat Level, including definitions and response guidelines for each of the alert levels, please review the Threat Advisory System.

You must have Cyware Access to reach the Threat Advisory System document. Contact membership@h-isac.org for access to Cyware.

Reference(s)	Info Security Magazine, Synopsys, Health-ISAC, Bleeping Computer, Health IT Security, Reuters, SonicWall, Bleeping Computer, Health-ISAC, Info Security Magazine, Info Security Magazine

Alert ID 66cc5013

View Alert

Tags DCH

TLP:GREEN Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.

Access the Health-ISAC Intelligence Portal Enhance your personalized information-sharing community with improved threat visibility, new notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more update and alerts, visit: **https://health-isac.cyware.com**