NETWORK INTELLIGENCE

The Digital Security Company

December 2023, Edition

SECURITY ADVISORY DIGEST

IN THIS EDITION:

Security Advisory Listing

- 🔴 Mr. Cooper, First American and Fidelity National Financial suffered data breach incidents.
- 🟠 Terrapin Attack Unveiled: OpenSSH Security at Risk.
- 🟡 Darwinbox on the Line: Alleged Cybersecurity Incident Sparks Investigation.
- 🟡 Anonymous Sudan Announces Cyber Attack on UAE Amid COP28 Preparations.

Also Inside

Security Patch Advisory

🔴 Critical 🟡 High 🟢 Low

Date: Dec 28, 2023

Mr. Cooper, First American and Fidelity National Financial suffered data breach incidents.

RECOMMENDATIONS

1. Conduct regular audits of the organization's cybersecurity infrastructure to identify vulnerabilities and weaknesses. This includes reviewing network configurations, access controls, and data encryption protocols.

2. Provide comprehensive cybersecurity training to employees to educate them about potential threats such as phishing and social engineering attacks. Ensure that employees understand their role in maintaining a secure environment.

3. Implement robust data encryption mechanisms to safeguard sensitive information. This includes encrypting data both in transit and at rest, making it more challenging for unauthorized parties to access and misuse.

4. Develop and regularly update an incident response plan that outlines the steps to be taken in the event of a cybersecurity incident. This plan should include communication protocols, system shutdown procedures, and coordination with relevant authorities.

5. Establish clear and timely communication protocols for notifying customers in the event of a data breach. Transparency and openness contribute to building trust, and customers should be informed about the steps they can take to protect themselves.

6. Implement strong identity and access management practices to control and monitor user access to sensitive data. This includes enforcing the principle of least privilege, regularly reviewing access permissions, and promptly revoking access for terminated employees.

7. Invest in dark web monitoring services to track the potential exposure of compromised data. Continuous surveillance can provide early detection of attempts to exploit or sell stolen information.

8. Implement robust data backup and recovery plans to ensure the availability of critical data in the event of a ransomware attack or data loss.

INTRODUCTION

Mr. Cooper suffered a massive data breach incident due to the ransomware attack: Mr. Cooper Group Inc., formerly Nationstar Mortgage Holdings Inc., is one of the largest mortgage servicers in the United States, with a servicing portfolio of approximately $937 billion and more than 4.3 million customers. The company suffered a ransomware attack on October 31. The incident caused a days-long outage for the company, including its public website and payment systems. In December 2023, the company started sending data breach notifications to impacted customers. According to the notice, hackers had unauthorized access to certain systems between October 30, 2023, and November 1, 2023. The breach exposed sensitive personal info such as full names, addresses, phone numbers, SSNs, DoB, and bank account numbers of 14,690,284 individuals. Currently, there are no specific details regarding how the attack was carried out, and no ransomware groups have claimed responsibility for the breach.

First American Financial Corporation hit by cyberattack: First American Financial Corporation is the second-largest title insurance company in America that provides title insurance and settlement services to the real estate and mortgage industries. On December 21, the company stated that it had experienced a cybersecurity incident. In response to the incident, the company took certain systems offline, including the email system. The company is still investigating the incident and is yet to determine the identity of the threat group, the type of attack & its TTPs and whether any data was stolen during the breach.

Fidelity National Financial hit by ALPHV/BlackCat ransomware gang: Fidelity National Financial (FNF), a major player in the U.S. insurance sector, has fallen victim to a cyberattack, resulting in a significant data breach affecting more than 1.3 million customers of its subsidiary, LoanCare. Attackers, identified as the notorious ALPHV ransomware gang, breached FNF's servers in mid-November, leading to the compromise of sensitive customer details. The compromised information includes customer names, addresses, Social Security numbers (SSNs), and loan numbers.

The above incidents pose a risk of phishing, scams, and social engineering attacks for affected individuals, with potential threats of bank fraud and identity theft due to the leaked bank account numbers.

REFERENCES

1. Mortgage giant Mr. Cooper data breach affects 14.7 million people
2. Fidelity National Financial attack exposes more than 1.3M subsidiary customers
3. First American takes IT systems offline after cyberattack

SECURITY ADVISORY

To know more about our services reach us at info@niiconsulting.com or visit www.niiconsulting.com

Date: Dec 20, 2023

Terrapin Attack Unveiled: OpenSSH Security at Risk

IMPACT

Successful exploitation of the vulnerabilities enables attackers to downgrade the security of an SSH connection, deactivate certain countermeasures to keystroke timing attacks, or obtain a MitM position at the session layer, potentially leading to unauthorized access to sensitive systems and data.

RECOMMENDATIONS

1. Ensure Linux distributions such as Ubuntu, RedHat, SUSE and others are updated with the latest security patches.

2. Ensure AsyncSSH, LibSSH, OpenSSH, PuTTY, and Transmit are updated to the latest releases. These vulnerabilities are addressed in - AsyncSSH 2.14.2, libssh 0.10.6 and libssh 0.9.8, OpenSSH 9.6/9.6p1, PuTTY 0.80 and Transmit 5.10.4

INCIDENT BRIEFING

The Terrapin attack, developed by researchers from Ruhr University Bochum, capitalizes on weaknesses in the SSH transport layer protocol in conjunction with cryptographic algorithms and encryption modes introduced by OpenSSH over a decade ago.

These weaknesses are tracked as CVE-2023-48795, CVE-2023-46445 and CVE 2023-46446.

Exploitation of these vulnerabilities requires active Man-in-the-Middle capabilities that can intercept and modify the connection's traffic at the TCP/IP layer. Additionally, the connection must be secured by either ChaCha20 Poly1305 or CBC with Encrypt-then-MAC.

The attack technique involves manipulating sequence numbers during the handshake process and removing or modifying messages exchanged through the communication channel.

The attacks subsequently result in downgrading public key algorithms for user authentication or disabling defenses against keystroke timing attacks in OpenSSH 9.5. This attack lowers connection security by truncating important negotiation messages without detection by the client or server.

Administrators can identify vulnerable SSH clients or servers using the Terrapin vulnerability scanner, published by the research team on GitHub.

Unlike a typical software bug, patching the Terrapin vulnerability involves updating both clients and servers to protect against prefix truncation attacks.

AFFECTED PACKAGES

- • AsyncSSH, LibSSH, OpenSSH, PuTTY, Transmit.

REFERENCES

1. Terrapin attacks can downgrade security of OpenSSH connections
2. SSH vulnerability exploitable in Terrapin attacks (CVE-2023-48795)
3. Terrapin Attack

SECURITY ADVISORY

To know more about our services reach us at info@niiconsulting.com or visit www.niiconsulting.com

Date: Dec 12, 2023

Darwinbox on the Line: Alleged Cybersecurity Incident Sparks Investigation

RECOMMENDATIONS

1. Implement encryption protocols for sensitive data, both in transit and at rest. This adds an additional layer of protection, especially if unauthorized access occurs.

2. Conduct regular security audits and vulnerability assessments to identify and address potential weaknesses in the IT infrastructure.

3. Provide comprehensive cybersecurity training to employees, emphasizing the importance of recognizing and reporting suspicious activities. Human error is a common entry point for cyberattacks, and informed staff can act as a crucial line of defense.

4. Implement multi-factor authentication across systems to add an additional layer of identity verification.

5. Clearly communicate data privacy policies to customers and ensure compliance with relevant data protection regulations. This builds trust and informs customers about the measures in place to protect their personal information.

6. Keep all software, including browsers, operating systems, and security software, up to date with the latest patches.

7. Consider investing in cybersecurity insurance to mitigate potential financial losses resulting from a data breach.

8. Regularly assess the security measures of third-party applications and services integrated into the organization's infrastructure. Ensure that vendors follow robust security practices.

INCIDENT BRIEFING

A threat actor named "dawnofdevil" on BreachForums claims to have breached Darwinbox Digital Solutions Pvt Ltd.

Darwinbox is an India-based human resources (HR) technology platform that provides a comprehensive suite of HR solutions to help organizations streamline their HR processes, enhance employee engagement, and make data-driven decisions.

The threat actor is offering unauthorized VPN access to Darwinbox for a $2,000 price tag. Access to compromised VPN credentials can be leveraged to infiltrate crucial systems, including Gitlab, Jira, Jenkins, and Confluence.

The alleged cyberattack, if valid, could pose a significant risk to Darwinbox's day-to-day operations, potentially allowing unauthorized entry to crucial systems essential for software development, project management, and internal collaboration.

Currently, the company's website remains accessible, raising questions about the legitimacy of the cyberattack.

LESSON LEARNED

The potential impact of this security threat extends beyond the company, impacting the broader cybersecurity landscape in India and the Asia & Pacific (APAC) region. It underscores the urgency for organizations to adopt proactive cybersecurity measures, emphasizing continuous assessment, and reinforcement of security protocols to mitigate risks and protect sensitive information.

REFERENCES

1. Darwinbox Allegedly Hit by Cyberattack; Threat Actor Demands US$2,000 for Access

SECURITY ADVISORY

To know more about our services reach us at info@niiconsulting.com or visit www.niiconsulting.com

Date: Dec 02, 2023

Anonymous Sudan Announces Cyber Attack on UAE Amid COP28 Preparations

RECOMMENDATIONS

1. Prioritize remediating known exploited vulnerabilities.

2. Implement Anti-DDoS measures on both On-premise and cloud for real-time DDoS attack prevention.

3. Utilize content delivery networks (CDNs) to distribute traffic.

4. Implement bot-detection technologies and algorithms -to identify large-scale web requests from botnets employed by actors to conduct DDOS Attacks.

5. Make sure your sites' infrastructure is up to date with the latest patches. If you're using WordPress, make sure plugins and themes are updated as well.

6. Scan your site for vulnerabilities to verify no patches are missing.

7. Make sure your WAF service/appliance is updated with the latest signatures. If possible, enable geolocation and restrict traffic to valid locations.

8. Microsoft customers can use layer 7 protection services such as Azure Web Application Firewall (WAF) (available with Azure Front Door, Azure Application Gateway) to protect web applications.

9. If possible, implement IP address access control lists (ACLs) in order to restrict access to Internet-facing systems.

10. Use strong passwords and enforce multi factor authentication wherever possible.

11. Apply the principle of least privilege to all systems and services so that users only have the access they need to perform their jobs.

INTRODUCTION

In a concerning turn of events, Anonymous Sudan has publicly declared its intent to launch a significant cyberattack on the United Arab Emirates (UAE). The group has not disclosed specific targets within the UAE, heightening the urgency for organizations and individuals across the region to fortify their cybersecurity defenses.

In the latest campaign against the UAE, Anonymous Sudan has singled out Dubai Airports as the initial focal point of their actions.

This cyber threat comes at a critical juncture, coinciding with the UAE's preparations to host the COP28 summit. This highlights the entangled link between geopolitical tensions and cyber warfare.

Escalating Cyber Warfare Landscape in the Middle East:

The Middle East is witnessing a surge in cyber warfare, with hacktivist groups intensifying their focus on Saudi Arabia and the UAE, driven by the longstanding tensions surrounding the Palestine-Israel conflict.

The UAE, despite its robust cyber defense infrastructure, finds itself under siege ahead of COP28, with key targets including the Higher Colleges of Technology, Federal Authority for Human Resources, Emirates News Agency (WAM News), Ministry of Economy, UAE Pass, Ministry of Justice, and Ministry of Health.

Meanwhile, Saudi Arabia has experienced a notable increase in cyber-attacks involving hacktivist groups such as Infinite Insight, Ganosec, and Team_R70. Major targets include the Ministry of Interior, Snap Saudi, Saudi Bin Salman Animal Product Company, Takaful Social Association for Care of Science Students, and BankAlbilad Saudi Arabia.

The operational methods employed by these groups primarily consist of DDoS attacks, website defacement, and attempts at data leaks. Despite limited successful data breaches, misinformation surrounding these incidents is rampant.

REFERENCES

1. Cyber Threat Alert: Anonymous Sudan Announces cyber attack on UAE
2. Cybersecurity Alert: The Middle East's Digital Battleground

SECURITY ADVISORY

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

11th Dec 2023 – 17th Dec 2023
TRAC-ID: NII23.12.0.3

UBUNTU

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Ubuntu Linux	**USN-6500-2: Squid vulnerabilities**	• Ubuntu 18.04 ESM • Ubuntu 16.04 ESM	**Kindly update to fixed version**
Ubuntu Linux	**USN-6546-1: LibreOffice vulnerabilities**	• Ubuntu 23.10 • Ubuntu 23.04	**Kindly update to fixed version**

ORACLE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Oracle Linux	**ELSA-2023-7791**	• Oracle Linux 9 (aarch64) • Oracle Linux 9 (x86_64)	**Kindly update to fixed version**
Oracle Linux	**ELSA-2023-7784**	• Oracle Linux 9 (aarch64) • Oracle Linux 9 (x86_64)	**Kindly update to fixed version**

SECURITY ADVISORY

To know more about our services reach us at info@niiconsulting.com or visit www.niiconsulting.com

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

11th Dec 2023 – 17th Dec 2023
TRAC-ID: NII23.12.0.3

IBM

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
IBM AIX	Security Bulletin: Multiple vulnerabilities in cURL libcurl affect AIX	• AIX 7.3.1, 7.3.2	**Kindly update to fixed version**
IBM Security Guardium	Security Bulletin: IBM Security Guardium is affected by multiple vulnerabilities	• IBM Security Guardium 11.5	**Kindly update to fixed version**

ADOBE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Adobe Prelude	**APSB23-67 : Security update available for Adobe Prelude**	• Adobe Prelude 22.6 and earlier versions	**Kindly update to fixed version**

SECURITY ADVISORY

To know more about our services reach us at info@niiconsulting.com or visit www.niiconsulting.com