NETWORK INTELLIGENCE

The Digital Security Company

October 2023, Edition

SECURITY ADVISORY DIGEST

IN THIS EDITION:

Security Advisory Listing

- Boeing Hacked by LockBit Ransomware Gang, Sensitive Data in Peril.
- Massive Breach Exposes Aadhaar Data of Millions of Indian Residents on the Dark Web.
- Electronics manufacturing firm Volex suffers cyber-attack.
- Cl0p actors hit Sony via MOVEit vulnerability

Also Inside

Security Patch Advisory

🔴 Critical 🟡 High 🟢 Low

Date: Oct 30, 2023

Boeing Hacked by LockBit Ransomware Gang, Sensitive Data in Peril

RECOMMENDATIONS

1. Ensure to apply latest security patch or use latest version of the third-party software.

2. Ensure to keep operating system patched with latest security updates.

3. Avoid sharing or storing sensitive data on third-party file sharing service.

4. Ensure Remote Desktop (RDP), Remote Procedure Call (RPC), and Virtual Network Computing (VNC) Services are strictly isolated from internet facing cloud or on-premises IT infrastructure. And ensure these remote services are only allowed through VPN tunnels.

5. Generate Canary Files which can help detect and identify a ransomware infection as immediately as possible and rapidly inform users if their network has been infiltrated.

6. Ensure to change password every 30-45 days and ensure to assign strong and complex password for the account.

7. Use a password manager to maintain strong and unique passwords.

8. Enable multi-factor authentication if its currently not in use and use secure MFA method, such as a hardware security key or an authentication app.

9. Ensure network segmentation is done properly and ensure sensitive data hosting servers are completely isolated from other networks or systems.

10.Always follow Zero-Trust approach in all aspect of business operations and activities, including cybersecurity operation and management.

11.Ensure to be more vigilant while communicating over email or phone call, to eliminate risk of social engineering like phishing.

INCIDENT BRIEFING

Leading aerospace and defense contractor, Boeing is the latest target of the Russian-linked LockBit ransomware gang. The cybercriminals posted Boeing as their newest conquest on their dark leak site. Boeing has yet to confirm the breach, stating they are assessing the claim.

LockBit claims to possess a substantial amount of sensitive data and threatens to publish it if Boeing does not contact them by a November 2nd deadline. The aerospace giant has not disclosed the amount of data allegedly exfiltrated, but it is estimated to be a significant amount.

The attackers say they exploited a zero-day vulnerability to breach the company. The LockBit group has a history of over 1,400 attacks worldwide and is known for its LockBit 3.0 ransomware variant.

The LockBit gang typically gains initial access to victim networks via remote desktop protocol (RDP) exploitation, drive-by compromise, phishing campaigns, abuse of valid accounts, and exploitation of public-facing applications.

This latest incident follows LockBit's recent attack on technology services giant CDW, where a reported $80 million ransom demand was met with a counteroffer of $1 million from the victimized company.

LESSON LEARNED

• Lack of endpoint security, use of admin account, using unpatched operating system, usage of commonly used passwords, reuse of same passwords across different platforms and failed to comply with security practices, often allows attackers to gain initial access onto the organization network and cause further damage.

REFERENCES

- LOCKBIT RANSOMWARE GANG CLAIMS TO HAVE STOLEN DATA FROM BOEING
- Boeing claimed by LockBit ransom gang
- Boeing assessing Lockbit hacking gang threat of sensitive data leak

SECURITY ADVISORY

Date: Oct 25, 2023

Massive Breach Exposes Aadhaar Data of Millions of Indian Residents on the Dark Web

RECOMMENDATIONS

1. Implement robust data encryption to protect sensitive information. Use access controls and authentication mechanisms to restrict access to critical databases.

2. Conduct regular security audits and vulnerability assessments to identify weaknesses in your security infrastructure.

3. Biometric data requires special protection. Ensure that it is stored and transmitted securely. Implement multi-factor authentication for accessing biometric data.

4. Employ data loss prevention (DLP) solutions to monitor and prevent data leakage.

5. Strengthen authentication methods for sensitive systems. Enforce strong password policies and regularly update credentials.

6. Train employees and users on cybersecurity best practices. Make them aware of the risks of sharing personal data online.

7. Ensure compliance with data protection and privacy laws, such as GDPR in Europe or data protection regulations in India. Regularly review and update policies to remain compliant with changing regulations.

8. Ensure that third-party vendors or partners adhere to strong security standards. Review and assess their security measures to protect shared data.

9. Implement the principle of least privilege (PoLP) to restrict access to only those who need it. Regularly review and revoke access for users who no longer require it.

10.Encourage users to report any suspicious activities or potential data breaches. Establish a clear communication channel for reporting security incidents.

11.Maintain regular backups of sensitive data and establish a recovery plan in case of data loss. Regularly test the backup and recovery processes.

INCIDENT BRIEFING

In a concerning revelation, hundreds of millions of personally identifiable information (PII) records, including Aadhaar cards of Indian residents, are currently available for sale on the Dark Web.

Resecurity's HUNTER unit discovered this alarming breach, coinciding with a Moody's report that raised concerns about the Aadhaar system's biometric authentication controls and security vulnerabilities. While the Indian government refuted the report's findings, evidence on the Dark Web suggests otherwise.

On Oct 09, a threat actor going by the name 'pwn0001' was spotted selling 815 million "Indian Citizen Aadhaar & Passport" records for $80,000 on the Breach Forums. The post claims the data set contains names, fathers' names, phone numbers, passport numbers, Aadhaar numbers, age, gender, address, district, Pincode, state, etc.

With India's Aadhaar system serving as one of the world's largest biometric ID programs, its breach poses a significant risk of digital identity theft and cyberenabled financial crimes.

LESSON LEARNED

- The incident highlights the growing risks associated with digital identity and the need for enhanced protection, especially as more services and processes become digitally reliant.
- Many Indian citizens are likely unaware that their data is being traded on the Dark Web. This incident emphasizes the need for public awareness and education on cybersecurity and digital identity protection

REFERENCES

- PII BELONGING TO INDIAN CITIZENS, INCLUDING THEIR AADHAAR IDS, OFFERED FOR SALE ON THE DARK WEB
- PII Belonging To Indian Citizens, Including Their Aadhaar IDs, Offered For Sale On The Dark Web

SECURITY ADVISORY

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

Date: Oct 12, 2023

Electronics manufacturing firm Volex suffers cyber-attack.

RECOMMENDATIONS

1. Promptly apply security patches and updates to all software and systems to address known vulnerabilities.

2. Regularly back up critical data and systems to offline or secure locations. Test backup and recovery procedures to ensure data can be restored quickly in case of ransomware or data loss.

3. Implement network segmentation to isolate critical systems and limit the lateral movement of attackers within the network.

4. Conduct regular cybersecurity awareness training for employees to recognize phishing attempts and other social engineering tactics.

5. Enforce the principle of least privilege (PoLP) to restrict user access rights and permissions.

6. Implement strong authentication methods, such as multi-factor authentication (MFA), for accessing sensitive systems.

7. Encrypt sensitive data at rest and in transit to protect it from unauthorized access.

8. Implement data loss prevention (DLP) solutions to monitor and control the movement of sensitive data.

9. Implement UBA solutions to analyze user behavior for signs of insider threats or compromised accounts.

10.Ensure compliance with relevant government regulations and industry standards for data protection and cybersecurity.

INCIDENT BRIEFING

Volex is a U.K.-based leading integrated manufacturing specialist for performance-critical applications and a supplier of power products. The company operates from 27 manufacturing locations with a global workforce of over 11,500 people across 24 countries.

On Oct 09, Volex disclosed that it was a victim of a cyber incident that resulted in unauthorized access to certain IT systems and data at some of the Group's international sites.

Despite the breach, all global production sites continue to operate with minimal disruption. Volex states that it has taken swift security measures and engaged third-party experts to investigate the breach further. While the exact details of the incident, including how the intrusion occurred and whether any ransom demands were made, remain undisclosed, the company is actively managing the situation and expects no significant financial impact.

The breach announcement caused Volex's shares to drop by over 3 percent, highlighting the potential consequences of cyberattacks on industrial entities.

LESSON LEARNED

- The cyberattack highlights the need for robust cybersecurity measures in safeguarding critical infrastructure, especially Operational Technology (OT), Industrial Internet of Things (IIoT), and Industrial Control Systems (ICS). Also, it emphasizes the importance of patching procedures and network segmentation to prevent malware movement and protect vital assets.

REFERENCES

- UK Power and Data Manufacturer Volex Hit by Cyberattack
- Manufacturing services tech giant hit with cyberattack

SECURITY ADVISORY

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

Date: Oct 06, 2023

Cl0p actors hit Sony via MOVEit vulnerability

RECOMMENDATIONS

1. Ensure MOVEit Transfer is updated with the latest security patches.

2. Use YARA rule to detect the ASPX web shell backdoors that are dropped during the attack.

3. Search for a user named Health Check Service within the MOVEit user database. Examine active sessions within the MOVEit database for user Health Check Service.

4. Rotate passwords and other secrets for accounts that are present within the MOVEit application to revoke access from potentially exposed credentials.

5. Additionally, security questions and MFA should also be configured for accounts that use the MOVEit Transfer application.

6. Search for and analyze any unexpected files in the c:\MOVEit Transfer\wwwroot\ folder. In particular, examine:

➢ Dynamic server code files such as aspx, php, and jsf
➢ Existence of human2.aspx (Note: human.aspx is the original aspx file used by MOVEit).
➢ Large files
➢ Files with recent creation timestamps.

7. On the MOVEit Transfer server, look for new files created in the C:\Windows\TEMP\[random]\ directory with a file extension of [.]cmdline

8. Review system admin, admin, file admin and group admin accounts - disable or delete accounts for people no longer using MOVEit or unrecognized accounts.

9. Ensure MOVEit security web headers are enforced.

10. Use the MOVEit Transfer Config Utility to validate system Paths, Filesystem settings, SSL/TLS settings, and SSH and FTP protocol settings.

11. Keep all systems and software updated to the latest patched versions.

INCIDENT BRIEFING

Sony Interactive Entertainment (SIE) has joined the list of 2000+ companies impacted by the MOVEit hacks. On June 22, the Cl0p ransomware group added Sony Group (sony[.]com) to their victim list along with three other companies (i.e., Andesa Services Inc., EY and PwC). Following this, the RansomedVC group also claimed to have data allegedly stolen from Sony.

On Oct 03, Sony sent data breach notifications to the affected individuals, confirming that the intrusion occurred after an unauthorized party exploited zero-day vulnerabilities in the MOVEit Transfer platform. The company says the hackers stole data on current and former employees and their families. According to a letter Sony filed with US authorities, the breach occurred in late May. The breach incident impacted almost 7,000 people. Threat actors claim to have stolen details for the SonarQube platform, certificates, Creators Cloud, incident response policies, a device emulator for generating licenses, Java source code files, Eclipse IDE screenshots and more.

According to KonBriefing, as of October 05, the number of known victims of the MOVEit attack is 2234 organizations, and affected individuals is 61.5 - 64.4M.

LESSON LEARNED

- Vulnerability or misconfiguration issues in software and inadequate security control, often allows attackers to have easy access to sensitive data or gain initial access to cause further damages to cloud-based or onpremises IT Infrastructure.

REFERENCES

- Sony confirms data breach impacting thousands in the U.S.
- Sony Confirms Data Breach Via MOVEit Vulnerability, Over 6000 Employees Impacted
- Sony confirms server security breaches that exposed employee data

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

25th Sept 2023 – 15th Oct 2023
TRAC-ID: NII23.10.0.1

UBUNTU

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Ubuntu Linux	**USN-6190-2: AccountsService vulnerability**	• Ubuntu 18.04 ESM • Ubuntu 16.04 ESM • Ubuntu 14.04 ESM	**Kindly update to fixed version**
Ubuntu Linux	**USN-6365-2: Open VM Tools vulnerability**	• Ubuntu 18.04 ESM • Ubuntu 16.04 ESM	**Kindly update to fixed version**

ORACLE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Oracle Linux	**ELSA-2023-5477**	• Oracle Linux 7 (aarch64) • Oracle Linux 7 (x86_64)	**Kindly update to fixed version**
Oracle Linux	**ELSA-2023-5683**	• Oracle Linux 8 (aarch64) • Oracle Linux 8 (x86_64)	**Kindly update to fixed version**

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

25th Sept 2023 – 15th Oct 2023
TRAC-ID: NII23.10.0.1

IVANTI

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Ivanti Endpoint Manager	SA-2023-08-08-CVE-2023- 35084	• EPM 2022 SU3 and all previous versions	**Kindly update to fixed version**
Ivanti Endpoint Manager	SA-2023-08-08-CVE-2023- 35083	• EPM 2022 SU3 and all previous versions	**Kindly update to fixed version**

TENABLE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Security Center	**[R1] Security Center Version 6.2.0 Fixes Multiple Vulnerabilities**	• Security Center 6.1.1 and earlier	**Kindly update to fixed version**

SECURITY ADVISORY