NETWORK INTELLIGENCE
The Digital Security Company

February 2024, Edition

SECURITY ADVISORY DIGEST

IN THIS EDITION:

Security Advisory Listing

- 🔴 Healthcare giant Change Healthcare grapples with major cyberattack.
- 🟡 Multiple vulnerabilities in Google Chrome.
- 🔴 Bank of America alerts customers of data breach after Infosys McCamish systems hack.
- 🟡 EventLogCrasher: A 0-day bug that lets authenticated actors crash the Windows Event Log service.

Also Inside

Security Patch Advisory

🔴 Critical 🟡 High 🟢 Low

Date: Feb 27, 2024

Healthcare giant Change Healthcare grapples with major cyberattack.

RECOMMENDATIONS

1. Ensure to update on-premises ScreenConnect instances to v23.9.8 or above immediately.

2. American Hospital Association (AHA) recommends that all health care organizations that were disrupted or are potentially exposed by this incidentt consider disconnection from Optum until it is independently deemed safe to reconnect to Optum.

3. Healthcare organizations should use this opportunity to test the security, redundancy and resiliency of their network and data backups ensuring they remain offline.

4. Ensure that all high criticality, known and exploited vulnerabilities have been patched, especially any which are internet facing.

5. Review and test cyber incident response plans, ensure they are well coordinated and integrated with emergency management plans. Test callout for activation of incident command structure and backup communications plans should email and VoIP communications fail.

6. Review business and clinical continuity downtime procedures to ensure mission critical and life critical functions could sustain a loss of information, operational and medical technology for up to 30 days.

7. Consider designating clinical downtime “coaches” and “safety officers” for each shift. These would be individuals who are experienced and adept at working with downtime, manual procedures should there be a loss of access to the EMR and other medical technology, and who could guide and lead other less experienced staff in the implementation of downtime procedures to ensure continuation of safe and quality care.

INCIDENT BRIEFING

Amidst a landscape of growing cyber threats, Change Healthcare, a cornerstone in U.S. healthcare technology, finds itself ensnared in a major cyberattack.

The assault, described as an "enterprise-wide connectivity issue," has forced the company into immediate action, disconnecting systems to contain the breach.

While specifics of the attack remain undisclosed, its repercussions are felt nationwide, disrupting healthcare services and pharmacy operations.

Change Healthcare's parent company, UnitedHealth Group (UHG), assures that the issue is isolated to its subsidiary, but the broader impact underscores the vulnerability of critical healthcare infrastructure.

In the latest article, BleepingComputer disclosed that the attack more likely exploited a critical ScreenConnect auth bypass flaw (CVE-2024-1709) and deployed BlackCat ransomware.

As cybersecurity experts scramble to contain the breach, the incident serves as a stark reminder of the urgent need for enhanced measures to protect patient data and ensure the continuity of essential healthcare services.

LESSON LEARNED

- The incident underscores the critical importance of robust cybersecurity measures, especially for organizations handling sensitive healthcare data. It highlights the need for constant vigilance and investment in cybersecurity infrastructure to fend off evolving threats.

- The widespread disruption caused by the attack illustrates the interconnected nature of healthcare systems. A cyberattack on one entity can have cascading effects, impacting healthcare services nationwide. This emphasizes the need for collaborative efforts and information sharing within the healthcare industry to mitigate such risks effectively.

REFERENCES

1. UnitedHealth confirms Optum hack behind US healthcare billing outage
2. Major Cyberattack Disrupts US Healthcare Giant Change Healthcare
3. US health tech giant Change Healthcare hit by cyberattack
4. UnitedHealth subsidiary Optum hack linked to BlackCat ransomware

SECURITY ADVISORY

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

Date: Feb 22, 2024

Multiple vulnerabilities in Google Chrome.

IMPACT

Successful exploitation of these vulnerabilities could allow an attacker to bypass security mechanisms, execute arbitrary code, gain access to sensitive information, and plant spyware on the targeted system

RECOMMENDATIONS

1. Kindly update Google Chrome browser for Windows, Mac, Linux, and Android to the latest releases.

To verify if the Chrome browser is running latest release, go to Chrome menu > Help > About Google Chrome.

These vulnerabilities are fixed in Chrome browser versions
122.0.6261.57 for Linux & Mac,
122.0.6261.57/.58 for Windows,
122.0.6261.64 for Android, and
122.0.6261.62 for iOS.

2. Ensure to update Chromium-based browsers such as Microsoft Edge, Brave, Opera, and Vivaldi to their latest releases as and when they become available.

INTRODUCTION

Google has released updates to its Chrome browser for Windows, Mac, Linux, Android, and iOS to address 12 security issues.

These vulnerabilities are tracked as CVE-2024-1669, CVE-2024-1670, CVE2024-1671, CVE-2024-1672, CVE-2024-1673, CVE-2024-1674, CVE-2024-1675, and CVE-2024-1676.

These vulnerabilities exist in Google Chrome due to:

- There is out-of-bounds memory access in Blink.
- Use after-free in Mojo and Accessibility.
- Inappropriate implementation in Site Isolation, Content Security Policy, Navigation, and Navigation.
- Insufficient policy enforcement in Download.

A remote attacker can trick the victim into opening a specially crafted web page, and execute arbitrary code on the target system.

INTRODUCTION

- Google Chrome versions before 122.0.6261.57 for Linux and Mac.
- Google Chrome versions before 122.0.6261.57/.58 for Windows
- Google Chrome versions before 122.0.6261.64 for Android
- Google Chrome versions before 122.0.6261.62 for iOS

REFERENCES

1. Google Chrome 122 Update Addresses Critical Security Vulnerabilities

SECURITY ADVISORY

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

Date: Feb 16, 2024

Bank of America alerts customers of data breach after Infosys McCamish systems hack.

RECOMMENDATIONS

1. Strengthen vendor risk management processes by conducting thorough assessments of third-party vendors' security posture before engaging their services.

2. Encrypt sensitive data both in transit and at rest to mitigate the risk of unauthorized access in the event of a security breach. Implement strong encryption algorithms and key management practices to protect customer information from being compromised.

3. Enforce multi-factor authentication for accessing sensitive systems and applications, including vendor portals and interfaces.

4. Develop and regularly test incident response plans to ensure swift and effective response to security incidents.

5. Provide comprehensive cybersecurity training and awareness programs for employees, including those who interact with third-party vendors.

6. Stay updated on relevant regulatory requirements and industry standards governing data protection and cybersecurity practices.

7. Maintain a robust patch management system to ensure that all software, operating systems, and applications are up-to-date with the latest security patches. Regularly apply patches to address known vulnerabilities.

8. Implement user behavior analytics to monitor and analyze user activities on the network. This helps in identifying unusual or suspicious behavior that may indicate a security threat.

INCIDENT BRIEFING

Bank of America alerts customers about a data breach resulting from a hack on Infosys McCamish Systems (IMS), one of its service providers, last year. Personal information, such as names, addresses, social security numbers, dates of birth, and financial data including account and credit card numbers, was compromised. Details were disclosed to the Attorney General of Texas.

The breach occurred around November 3, 2023, when unauthorized access was gained to IMS systems, leading to the compromise of data related to Bank of America's deferred compensation plans. The LockBit ransomware gang claimed responsibility on November 4th, revealing that its operators encrypted over 2,000 systems during the attack. According to IMS breach notification letter to the Attorney General of Maine, 57,028 individuals were directly impacted by the breach.

Since September 2019, LockBit ransomware-as-a-service has targeted various notable organizations, including the UK Royal Mail, Continental automotive giant, the City of Oakland, and the Italian Internal Revenue Service. A joint advisory in June by cybersecurity authorities in the United States and global partners disclosed LockBit's extortion of over $91 million from U.S. organizations through about 1,700 attacks since 2020.

REFERENCES

1. Bank of America warns customers of data breach after vendor hack
2. Data Breach Notifications
3. Data breach affects 57,000 Bank of America accounts

SECURITY ADVISORY

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

Date: Feb 02, 2024

EventLogCrasher: A 0-day bug that lets authenticated actors crash the Windows Event Log service.

IMPACT

The immediate consequence of the Event Log service outage is operational disruption. With logging capabilities crippled, IT teams face challenges in monitoring system health, diagnosing issues, and investigating security incidents. The blackout creates a window of opportunity for adversaries to infiltrate networks, conduct reconnaissance, and execute advanced persistent threats undetected.

RECOMMENDATIONS

1. Ensure Windows servers and workstations are updated with the latest security patches. The 0patch micropatching service has released unofficial patches for most affected Windows versions on Wednesday, available for free until Microsoft releases official security updates to address the zero-day bug.

2. Monitor for unexpected shutdown of Windows Event Log service more than 2 times in a short duration of time. Crashing the Event Log service three times makes it persistently stopped.

INTRODUCTION

On January 23, security researcher Florian disclosed a new vulnerability named EventLogCrasher, which enables any authenticated user with network connectivity in a Windows environment (including in the Windows domain) to crash the Windows Event Log service.

Florian stated that according to MSRC, the bug does not meet the bar for servicing and published a proof-of-concept (PoC) after this.

According to the PoC, an attacker can send a malformed UNICODE_STRING object to the ElfrRegisterEventSourceW method exposed by the RPC-based EventLog Remoting Protocol and crash the wevtsvc!VerifyUnicodeString function inside the Event Log service.

According to the 0patch blog post, if you suspect someone intentionally crashed the Event Log service on one of our computers, it is recommended to attempt to rescue any potentially queued Security and System events by disconnecting the computer from the network and manually starting the Windows Event Log service. Next, it is recommended to reconnect the computer to the network to allow IDS/SIEM to collect them as well and inspect network traffic (incoming SMB connections to \pipe\eventlog) to see where the attack is coming from.

AFFECTED PRODUCTS

- The vulnerability affects all versions of Windows, from Windows 7 up to the latest Windows 11 and from Server 2008 R2 to Server 2022

REFERENCES

1. New Windows Event Log zero-day flaw gets unofficial patches
2. A zero-day vulnerability (and PoC) to blind defenses relying on Windows event logs

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

22nd Jan 2024 – 28th Jan 2024
TRAC-ID: NII24.01.0.4

UBUNTU

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Ubuntu Linux	**USN-6609-1: Linux kernel vulnerabilities**	• Ubuntu 22.04 LTS • Ubuntu 20.04 LTS	**Kindly update to fixed version**
Ubuntu Linux	**USN-6608-1: Linux kernel vulnerabilities**	• Ubuntu 23.10 • Ubuntu 22.04 LTS	**Kindly update to fixed version**

ORACLE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Oracle Linux	**ELSA-2024-12094**	• Oracle Linux 9 (aarch64) • Oracle Linux 9 (x86_64)	**Kindly update to fixed version**
Oracle Linux	**ELSA-2024-12093**	• 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

22nd Jan 2024 – 28th Jan 2024
TRAC-ID: NII24.01.0.4

IBM

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
IBM Security QRadar SIEM	IBM Disconnected Log Collector is vulnerable to using components with known vulnerabilities	• IBM Disconnected Log Collector v1.0 - v1.8.3	**Kindly update to fixed version**
IBM Security Guardium	IBM Security Guardium is affected by vulnerabilities in the Linux Kernel	• IBM Security Guardium 11.3 • IBM Security Guardium 11.4 • IBM Security Guardium 11.5 • IBM Security Guardium 12.0	**Kindly update to fixed version**

CENTOS

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
CentOS	**CESA2024:0343**	• Moderate CentOS 7 LibRaw 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