NETWORK INTELLIGENCE

The Digital Security Company

August 2023, Edition

SECURITY ADVISORY DIGEST

IN THIS EDITION:

Security Advisory Listing

- Multiple hacker groups targeted 1000+ Indian sites during Independence Day celebrations
- Remote code execution bug in WinRAR
- A flaw in Dell Storage Integration Tools for VMware (DSITV) exposes vCenter admin creds
- CERT-IN warns of multiple high severity vulnerabilities in Google Chrome

Also Inside

Security Patch Advisory

Critical High Low

Date: Aug 21, 2023

Multiple hacker groups targeted 1000+ Indian sites during Independence Day celebrations

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

9. Ensure PHPMyAdmin, MySQL server, Apache HTTP server, Apache Tomcat server, Confluence Server and Data Center are updated with latest security patches.

10.Use strong passwords and enforce multifactor 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

Indian officials disclosed that hacktivist groups targeted over 1,000 websites via DDoS attacks during the Independence Day celebrations last week, on August 15.

Targeted sectors: government agencies, education, BFSI, and small businesses.

Government and BFSI sectors experienced DDoS attacks, while education and small businesses experienced defacement attacks.

The attacks were part of OpIndia and were conducted by hacktivist groups from Pakistan, Bangladesh and other Muslim nations.

The attacks used compromised credentials, targeted known vulnerabilities in web servers and administrative panels, and used open-source HTTP flooding tools and proxy services to overwhelm target website servers temporarily.

REFERENCES

Hacktivists 'targeted' over 1,000 India sites during I-day celebrations

SECURITY ADVISORY

Date: Aug 21, 2023

Remote code execution bug in WinRAR

BUSINESS IMPACT

Successful exploitation of the vulnerability enables remote hackers to execute arbitrary code or commands and deploy further malware for disruptive operations.

INTRODUCTION

On Aug 02, RARLAB released a security update for its WinRAR compression utility to fix a high-severity vulnerability that could be abused to run malicious code remotely on user devices.

The vulnerability exists due to the out-of-bounds write issue in the RAR4 recovery volumes processing code. The threat actors can simply trick target users into visiting a malicious page or opening a specially crafted archive file and execute arbitrary commands.

CVSS Score: 7.8

RECOMMENDATIONS

1. Ensure to update WinRAR to version 6.23 or above.

AFFECTED PRODUCTS

- WinRAR versions before 6.23

REFERENCES

- WinRAR flaw lets hackers run programs when you open RAR archives
- RARLAB WinRAR Recovery Volume Improper Validation of Array Index Remote Code Execution Vulnerability

SECURITY ADVISORY

Date: Aug 14, 2023

A flaw in Dell Storage Integration Tools for VMware (DSITV) exposes vCenter admin creds

BUSINESS IMPACT

Successful exploitation of the vulnerability allows an attacker to steal vCenter admin credentials, execute arbitrary code, take control of a company's affected system, and deploy further malicious payload to execute ransomware-like disruptive attacks.

INTRODUCTION

Security researcher Tom Pohl discovered a hardcoded encryption key flaw (tracked as CVE-2023-39250) in Dell's Storage Compellent Integration Tools for VMware (CITV).

Dell's CITV software supports storage integration with VMware vCenter. However, it must be configured with VMware vCenter credentials to integrate the client. Only organizations that run these two services in collaboration are affected.

The flaw exists because Dell CITV uses a static AES encryption key (identical for all Dell customers across all installs) to encrypt the CITV configuration file containing the program's settings, including the entered vCenter admin credentials.

Malicious insiders or low-privileged external attackers having access to Dell CITV can exploit this vulnerability to decrypt stored vCenter admin credentials and retrieve the cleartext password.

Note: Dell Compellent reached its end of life in 2019.

RECOMMENDATIONS

Dell recommends:

1. Changing the default root password of all current appliances using Compellent DSITV

2. Ensuring users follow the process to change the default root password of all new appliances using Compellent DSITV

For instructions – CLICK HERE

LESSON LEARNED

- Dell Storage Integration Tools for VMware (DSITV) v06.01.00.016

REFERENCES

- Dell Compellent hardcoded key exposes VMware vCenter admin creds
- DSA-2023-282: Security Update for Dell Storage Integration Tools for VMware (DSITV) Vulnerabilities

SECURITY ADVISORY

Date: Aug 11, 2023

CERT-IN warns of multiple high severity vulnerabilities in Google Chrome

BUSINESS IMPACT

Successful exploitation of these vulnerabilities could allow an attacker to execute arbitrary code, bypass security restrictions or cause a denialof-service condition on the targeted system.

RECOMMENDATIONS

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

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

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

BUSINESS IMPACT

Google has released updates to its Chrome browser for Windows, Mac, Linux and Android to address 17 security fixes.

These vulnerabilities are tracked as CVE-2023-4068, CVE-2023-4069, CVE2023-4070, CVE-2023-4071, CVE-2023-4072, CVE-2023-4073, CVE-2023-4074, CVE-2023-4075, CVE-2023-4076, CVE-2023-4077 and CVE-2023-4078.

These vulnerabilities exist in Google Chrome for Desktop due to:

- Type Confusion in V8
- Heap buffer overflow in Visuals
- Out of bounds read and write in WebGL
- Out-of-bounds memory access in ANGLE
- Use after free in Blink Task Scheduling, Cast and WebRTC
- Insufficient data validation in Extensions
- Inappropriate implementation in Extensions

A remote attacker can trick the victim into opening a specially crafted web page, trigger out-of-bounds, use-after-free error or type confusion error and execute arbitrary code on the target system.

AFFECTED PRODUCTS

- Google Chrome versions prior to 115.0.5790.170 for Mac and Linux
- Google Chrome versions prior to 115.0.5790.170/.171 for Windows
- Google Chrome versions prior to 115.0.5790.166 for Android

REFERENCES

- Government issues high-risk warning for Google Chrome users, asks users to update browser immediately
- Govt issues high-severity warning for Google Chrome users

SECURITY ADVISORY

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

7th Aug 2023 – 13th Aug 2023
TRAC-ID: NII23.08.0.2

UBUNTU

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Ubuntu Linux	USN-6276-1: unixODBC vulnerability	• Ubuntu 16.04 ESM • Ubuntu 14.04 ESM	Kindly update to fixed version
Ubuntu Linux	USN-6267-2: Firefox regressions	• Ubuntu 20.04 LT	Kindly update to fixed version

ORACLE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Oracle Linux	ELSA-2023-4642	• Oracle Linux 9 (aarch64) • Oracle Linux 9 (x86_64)	Kindly update to fixed version
Oracle Linux	ELSA-2023-4644	• Oracle Linux 9 (aarch64) • Oracle Linux 9 (x86_64)	Kindly update to fixed version

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

7th Aug 2023 – 13th Aug 2023
TRAC-ID: NII23.08.0.2

GOOGLE CHROME

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Chrome for Mac, Linux and Windows	Stable Channel Update for Desktop	• Chrome versions prior to 116.0.5845.96 for Mac and Linux • Chrome versions prior to 116.0.5845.96/.97 for Window	**Kindly update to fixed version**
Chrome for iOS	Chrome Stable for iOS Update	• Chrome versions prior to 116.0.5845.103 for iOS	**Kindly update to fixed version**

FORTINET

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
FortiOS	**FortiOS - Buffer overflow in execute extender command**	• FortiOS version 7.0.0 through 7.0.3 • FortiOS 6.4 all versions • FortiOS 6.2 all version	**Kindly update to fixed version**

SECURITY ADVISORY