NETWORK INTELLIGENCE

The Digital Security Company

July 2022, Edition 1.0

SECURITY ADVISORY DIGEST

IN THIS EDITION:

Security Advisory Listing

- Robin Banks, a new phishing-as-a-service platform, targets the customers of banks & online services
- Critical SQL injection bug in SonicWall GMS and Analytics On-Prem
- Microsoft Teams & multiple Microsoft 365 services with Teams integration suffered issues after a service outage lasting several hours
- XSS vulnerability in Microsoft Teams

Also Inside

Security Patch Advisory

Critical High Low

Date: July 28, 2022

Robin Banks, a new phishing-as-a-service platform, targets the customers of banks & online services

BUSINESS IMPACT

1. Block the threat indicators at their respective controls.

2. Ensure Microsoft Windows Workstations, Microsoft Exchange Server, SharePoint server, Microsoft SQL server and Microsoft IIS Server are updated with latest security patches.

3. Don't click on links sent through SMS and email, especially if asked to access your account or enter your credentials.

4. Use a password manager to ensure the use of unique credentials across all accounts.

5. Enable multi-factor authentication (MFA) for all accounts.

6. Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.

7. Regularly change passwords to network systems, accounts, and avoid reusing passwords for different accounts.

8. Maintain offline backups of data and regularly maintain backup and restoration.

9. Keep all operating systems and software up to date. Prioritize patching known exploited vulnerabilities.

10. Remove unnecessary access to administrative shares, especially ADMIN$ and C$.

11. Block public facing Remote Desktop Protocol (RDP). Suppose remote access to RDP or terminal services is required; in that case, it should only be made accessible through a secure Virtual Private Network (VPN) connection (with Multi-Factor Authentication) to the corporate network or through a zero-trust remote access gateway.

12. Use application directory allowlisting on all assets to ensure that only authorized software can run, and all unauthorized software is blocked from executing.

13. 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

Robin Banks is a new phishing-as-a-service (PhaaS) platform project, active since March 2022. The platform offers ready-made phishing kits to cyber-criminal actors aiming to gain access to the financial information of individuals residing in the U.S., the U.K., Canada, and Australia.
Robin Banks platform has advertised that threat actors can choose from a myriad of brands to impersonate and target the customers of financial institutions including Bank of America, Capital One, Citibank, Wells Fargo, as well as international companies like Lloyds Bank of England, Netflix in Canada, and Commonwealth Bank in Australia. Robin Banks also offers templates to steal Microsoft, Google, Netflix, and T-Mobile accounts.

DOMAINS

Robinbanks[.]in
Robinbnks[.]in
robinbanks[.]cc
auth21c-verify[.]com
Rbpages[.]nl
Rbpagev2[.]in
Rbresults[.]pm

IP's

185.61.137[.]142
5.206.227[.]166

REFERENCES

- New 'Robin Banks' phishing service targets BofA, Citi, and Wells Fargo
- Robin Banks might be robbing your bank

SECURITY ADVISORY

Date: July 25, 2022

Critical SQL injection bug in SonicWall GMS and Analytics On-Prem

BUSINESS IMPACT

Successful exploitation of the vulnerability allows a remote attacker to read, delete, and modify data in the database, bypass authentication and gain complete control over the affected application.

RECOMMENDATIONS

1. Kindly update SonicWall GMS and Analytics On-Prem to a latest fixed version.

2. Incorporate a Web Application Firewall, to block SQL injection attacks even on unpatched deployments.

INTRODUCTION

SonicWall has released fixes to address a critical security vulnerability (CVE- 2022-22280), impacting SonicWall GMS (Global Management System) and Analytics On-Prem products. The vulnerability allows a remote attacker to execute arbitrary SQL queries in a database. The security flaw is exploitable from the network without requiring authentication or user interaction, while it also has low attack complexity.

The vulnerability exists due to the Improper Neutralization of Special Elements used in an SQL Command that leads to unauthenticated SQL Injection attacks. A remote non-authenticated attacker can send a specially crafted request to the affected application and execute arbitrary SQL commands within the application database.

CVSS Score: 9.4

AFFECTED PRODUCT

- GMS 9.3.1-SP2-Hotfix1 and earlier versions
- Analytics 2.5.0.3-2520 and earlier versions

REFERENCES

- SonicWall: Patch critical SQL injection bug immediately
- Security Notice: SonicWall GMS SQL Injection Vulnerability

SECURITY ADVISORY

Date: July 22, 2022

Microsoft Teams & multiple Microsoft 365 services with Teams integration suffered issues after a service outage lasting several hours

BUSINESS IMPACT

Microsoft Teams & multiple Microsoft 365 services with Teams integration suffered issues after a service outage lasting several hours.

RECOMMENDATIONS

1. Ensure Microsoft Teams is updated with latest security patches.

INTRODUCTION

As per the global outage monitor Down Detector, users started facing issues with Microsoft Teams around 06:45 AM IST on July 21, 2022. The hour-long outage for tens of thousands of customers globally. According to Down Detector, more than 4,800 users in the United States and over 18,200 users in Japan were affected by the disruption.

Microsoft stated that a recent deployment contained a broken connection to an internal storage service, which caused the impact. We're working to direct traffic to a healthy service to mitigate the impact.
According to Microsoft 365 Service health status page, the outage affected the following services:

- Microsoft Teams (Access, chat, and meetings)
- Exchange Online (Delays sending mail)
- Microsoft 365 Admin center (Inability to access)
- Microsoft Word within multiple services (Inability to load)
- Microsoft Forms (Inability to use via Teams)
- Microsoft Graph API (Any service relying on this API may be affected)
- Office Online (Microsoft Word access issues)
- SharePoint Online (Microsoft Word access issues)
- Project Online (Inability to access)
- PowerPlatform and PowerAutomate (Inability to create an environment with a database)
- Autopatches within Microsoft Managed Desktop
- Yammer (Impact to Yammer experiments)
- Windows 365 (Unable to provision Cloud PCs)

Microsoft added on Twitter at 01:40 AM IST on July 22, 2022, that after redirecting traffic to a healthy service to mitigate the impact, its telemetry indicates no further instances of impact observed following the recovery actions.

REFERENCES

- Microsoft Teams outage also takes down Microsoft 365 services

SECURITY ADVISORY

Date: July 18, 2022

XSS vulnerability in Microsoft Teams

BUSINESS IMPACT

Successful exploitation of the vulnerability allows a remote attacker to bypass CSP, trigger XSS and launch HTML injection attacks.

RECOMMENDATIONS

1. Ensure Microsoft Teams is updated to latest version.

INTRODUCTION

A security researcher discovered a security flaw in Microsoft Teams that enable cross-site scripting (XSS) attacks by abusing the sticker feature. When a sticker is sent on Microsoft Teams, Teams will convert it as an image and then uploads it. The image is sent as “RichText/Html” in the message.

The vulnerability exists in the JavaScript element (angular-jquery) that could be utilized to bypass the CSP. An attacker can send a specially crafted iframe to create a malicious payload and send it via the stickers function in Teams to trigger XSS. The vulnerability allows potential HTML injection attacks against multiple domains.

Microsoft has patched the security issue in March 2022.

AFFECTED PRODUCT

- Microsoft Teams

REFERENCES

- Microsoft Teams security vulnerability left users open to XSS via flawed stickers feature

SECURITY ADVISORY

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

4th July to 10th July 2022
TRAC-ID: NII22.07.0.2

UBUNTU

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Ubuntu Linux	USN-5501-1: Django vulnerability	• Ubuntu 22.04 LTS • Ubuntu 21.10 • Ubuntu 20.04 LTS • Ubuntu 18.04 LTS	Kindly update to fixed version
Ubuntu Linux	USN-5479-2: PHP vulnerabilities	• Ubuntu 16.04 ESM	Kindly update to fixed version

ORACLE

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Oracle Linux	ELSA-2022-5526	• Oracle Linux 8 (aarch64) • Oracle Linux 8 (x86_64)	Kindly update to fixed version
Oracle Linux	ELSA-2022-9565	• Oracle Linux 6 (i386) • Oracle Linux 6 (x86_64)	Kindly update to fixed version

Security Patch Advisory

Severity Matrix			
L	M	H	C
Low	Medium	High	Critical

4th July to 10th July 2022
TRAC-ID: NII22.07.0.2

IBM

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
IBM WebSphere Application Server Libert	Security Bulletin: IBM WebSphere Application Server Liberty is vulnerable to Identity Spoofing (CVE-2022-22476)	• IBM WebSphere Application Server Liberty 17.0.0.3 - 22.0.0.7	**Kindly update to fixed version**
IBM WebSphere Application Server Liberty	Security Bulletin: IBM WebSphere Application Server Liberty is vulnerable to spoofing due to Eclipse Paho (CVE-2019-11777)	• IBM WebSphere Application Server Liberty 17.0.0.3 - 22.0.0.7	**Kindly update to fixed version**

BROADCOM (AKA, SYMANTEC)

TECHNOLOGIES	ADVISORIES	AFFECTED PRODUCTS	RECOMMENDATION
Advanced Secure Gateway, ProxySG	**Advanced Secure Gateway, ProxySG**	• Advanced Secure Gateway (ASG) versions 6.7, 7.3 • ProxySG versions 6.7, 7.3	**Kindly update to fixed version**

SECURITY ADVISORY