Subject: Web Server Compromise and Malware Distribution via JavaScript Injection Date: April 14, 2025 Reported by: MANJEESWAR KV, Cybersecurity Analyst

Incident Summary

The website yummyrecipesforme.com was compromised due to a brute force attack on the administrator account. The attacker successfully accessed the admin panel using a default password, allowing them to inject malicious JavaScript code into the site's source code.

The injected script prompted users to download an executable file, disguised as a browser update. Once run, the script redirected the browser to a malicious domain, greatrecipesforme.com, where further malware was hosted. The attacker then locked out the legitimate admin by changing the password.

Timeline of Events (Simplified)

Brute force login using default admin password.

Malicious JavaScript injected into website source code.

Users visit site → prompted to download malware.

Malware redirects browser to greatrecipesforme.com.

Users report slow performance and strange downloads.

Admin unable to log in; cybersecurity team begins investigation.

Technical Details

Protocols Used:

DNS – Resolving domain names (both legitimate and malicious).

HTTP – Delivering webpages and initiating downloads.

Attack Method:

Brute force attack exploited lack of rate limiting and weak credentials.

Client-side script injection used to deploy and trigger malware.

Result:

Customers exposed to malware.

Website reputation potentially damaged.

Admin access compromised.

Recommendations

To prevent future brute force attacks and improve overall security posture:

Change all default credentials immediately.

Implement account lockout after a number of failed login attempts.

Use strong, complex passwords and encourage regular changes.

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

Deploy a Web Application Firewall (WAF) to detect and block malicious behavior.

Conduct regular vulnerability scans and penetration tests.

Monitor file integrity and source code for unauthorized changes.

Log all login attempts, both successful and failed, for audit and alerting.