***Abstract* –this document provides a comprehensive analysis of critical security vulnerabilities in Mobile Device Management (MDM) solutions. The analysis covers various aspects of these vulnerabilities, including their technical details, potential attack vectors, and implications for security professionals and organizations across different industries.**

The analysis provides a high-quality summary of these vulnerabilities, offering valuable insights for security professionals, IT administrators, and other specialists. By understanding these vulnerabilities and their implications, organizations can better protect their MDM solutions, enhance their security posture, and mitigate the risks associated with these flaws. This document serves as a crucial resource for those looking to safeguard their mobile device management systems against sophisticated cyber threats.

I. FileWave MDM

FileWave MDM is a comprehensive multi-platform mobile device management solution that allows IT administrators to manage, monitor, and secure an organization's devices. It supports a wide range of devices, including iOS and Android smartphones, macOS and Windows tablets, laptops, workstations, and smart devices such as televisions.

FileWave MDM offers centralized management of all devices, enabling administrators to monitor and control them from a single interface. It includes several security features, such as data encryption, remote wipe capabilities, and password policies, which help protect devices and data from unauthorized access. The platform can be customized to fit the specific needs of an organization, allowing administrators to configure settings and policies as required. Additionally, FileWave MDM can automate many tasks, such as software updates and device configurations, saving time and reducing the risk of errors. It is compatible with a wide range of devices and operating systems, including macOS, Windows, iOS, iPadOS, tvOS, ChromeOS, and Android

A. Authentication Flaws

1) Vulnerabilities Identified:

- Two critical vulnerabilities, CVE-2022-34907 and CVE-2022-34906, were discovered in FileWave's mobile device management (MDM) system.
- CVE-2022-34907 is an authentication bypass flaw that allows attackers to gain super_user access.
- CVE-2022-34906 involves a hard-coded cryptographic key that can be exploited to gain unauthorized access.

2) Impact of Vulnerabilities:

- These vulnerabilities are remotely exploitable, enabling attackers to bypass authentication mechanisms and gain full control over the MDM platform and its managed devices.
- Attackers could exfiltrate sensitive data such as device serial numbers, user email addresses, full names, addresses, geo-location coordinates, IP addresses, and device PIN codes.
- Legitimate MDM capabilities could be abused to install malicious packages or executables and gain direct access to devices through remote control protocols.

3) Scope of Vulnerabilities:

- Over 1,100 vulnerable internet-facing FileWave servers were identified across various industries, including government agencies, educational institutions, and large enterprises.
- Each vulnerable instance contained an unrestricted number of managed devices, making them prime targets for potential attacks.

4) Exploitation Demonstration:

- Created a standard FileWave setup and enrolled six devices to demonstrate the vulnerability.
- Using the authentication bypass vulnerability, they were able to take full control over the MDM instance, exfiltrate data, and install malicious packages, including a fake ransomware virus.

5) Mitigation and Response:

- FileWave addressed these vulnerabilities in version 14.7.2 and has urged users to apply the update to mitigate the risks.
- The company has actively worked with customers to ensure that affected systems are patched or updated.
- Users are recommended to double-check that the security update is properly installed and up to date to avoid the risk of third-party attacks.

6) Security Measures:

- FileWave encrypts all customer content in-transit and at-rest.
- The platform supports a wide range of devices, including iOS and Android smartphones, macOS and Windows tablets, laptops, workstations, and smart devices such as televisions.
- The MDM web server, written in Python using the Django framework, handles device enrollment, retrieves device information, and supplies commands to devices.

B. *Technical details*

The key vulnerability lies in the hardcoded scheduler secret being accepted for authentication instead of proper admin credentials. The code changes in newer versions attempted to fix this but introduced a new bypass vector using the Host header.

- The vulnerability exists in the FileWave MDM web server component, written in Python using the Django framework. It exposes TCP ports 20443 and 20445.
- The web server handles client device enrollment, retrieves device information, and supplies commands to devices.
- For client devices, enrollment does not require authentication by default, though credentials can be enabled.
- For admin authentication, a username/password combination returns a valid token to control devices.
- A backend scheduler service uses a hardcoded shared secret to authenticate with the web server instead of admin credentials.
- In older versions (up to 13.1.3), supplying the hardcoded scheduler secret in the Authorization header would grant super_user privileges, bypassing authentication.
- In newer versions, FileWave added a middleware check comparing the Authorization header to the scheduler secret and checking if the Host header is localhost.
- By setting the Host header to localhost, an attacker can bypass the new middleware check and gain super_user privileges.
- Exploiting this vulnerability allows full control over the MDM instance, enabling attackers to control managed devices, exfiltrate sensitive data like usernames, emails, locations, and install malicious software.

C. *Attack*

1) *Setup and Initial Exploitation:*

- A standard FileWave setup was created, and six devices were enrolled.
- The MDM web server was exploited using the discovered vulnerability, allowing data leakage about all managed devices.
- Enrolled six devices (a mix of different operating systems and device types supported by FileWave MDM) to be managed by the MDM server.

2) *Exploiting the Authentication Bypass Vulnerability*

- Identified the MDM web server component, written in Python using the Django framework, exposing TCP ports 20443 and 20445.
- For older versions (up to 13.1.3), supplied the hardcoded scheduler secret in the Authorization header to gain super_user access, bypassing authentication.
- For newer versions, set the Host header to localhost and supplied the scheduler secret in the Authorization header to bypass the middleware check and gain super_user access

3) *Data Exfiltration:*

- Administrative access was gained by bypassing authentication on the MDM server.
- Information about the managed devices, including their operating systems, ecosystems, and settings, was exfiltrated.

4) *Malicious Package Installation:*

- Regular MDM functionality was used to install packages and software on managed devices.
- Malicious packages, including a fake ransomware virus, were installed on each controlled device.
- This demonstrated how an attacker could leverage FileWave's capabilities to take control over different managed devices and execute remote code.

5) *Demonstration of Potential Harm:*

The exploit showcased the severity and potential harm by demonstrating the ability to control all managed devices, exfiltrate sensitive data, and install malicious software.

D. *Exploitation Technical Flow: CVE-2022-34906*

This exploitation flow highlights how the hard-coded cryptographic key vulnerability in FileWave MDM could be leveraged by an unauthenticated attacker to gain unauthorized access, exfiltrate sensitive data, and potentially compromise the managed devices.

1) *Identifying the Vulnerability*

- FileWave MDM versions prior to 14.6.3 and 14.7.x before 14.7.2 used a hard-coded cryptographic key
- This hard-coded key did not change between different installations or versions of the FileWave MDM system.

2) *Exploiting the Hard-coded Key*

- An unauthenticated attacker could leverage the hard-coded cryptographic key to decrypt sensitive information stored in the FileWave MDM system.
- The attacker could also potentially send crafted requests to the devices managed by the MDM platform, abusing legitimate MDM capabilities.

3) *Gaining Unauthorized Access*

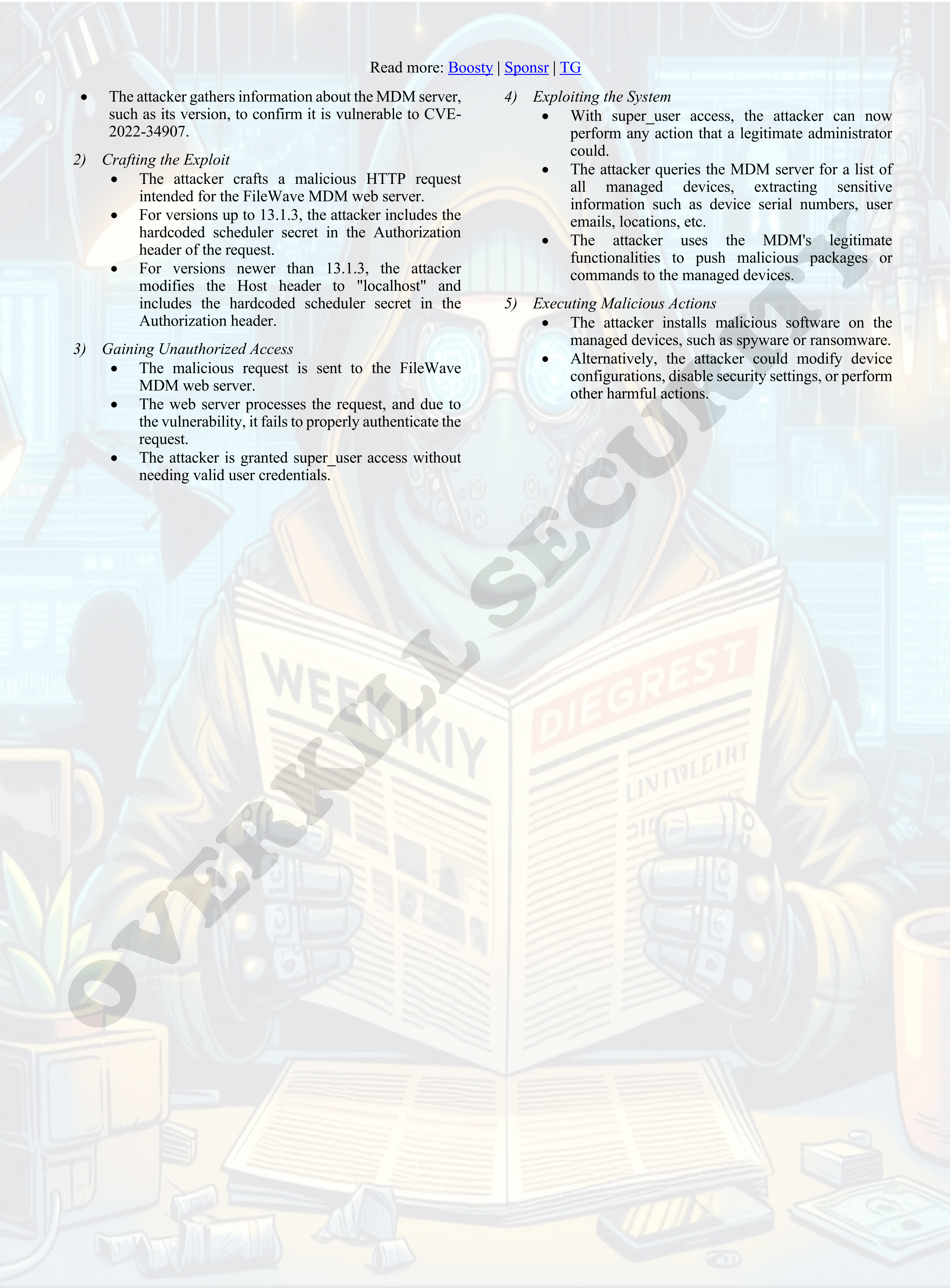
- By exploiting the hard-coded key vulnerability, an attacker could gain unauthorized access to the MDM platform and its managed devices.
- This could enable the attacker to exfiltrate sensitive data from the managed devices, including usernames, email addresses, IP addresses, geo-locations, and more.
- Additionally, the attacker could potentially install malicious software or execute arbitrary code on the managed devices by abusing the MDM's legitimate capabilities

E. *Exploitation Technical Flow: CVE-2022-34907*

For CVE-2022-34907, the authentication bypass vulnerability in FileWave MDM, the technical exploitation flow is as follows:

1) *Preparing the Attack*

- The attacker identifies a target FileWave MDM server that is accessible over the internet.



- The attacker gathers information about the MDM server, such as its version, to confirm it is vulnerable to CVE-2022-34907.

2) *Crafting the Exploit*
   - The attacker crafts a malicious HTTP request intended for the FileWave MDM web server.
   - For versions up to 13.1.3, the attacker includes the hardcoded scheduler secret in the Authorization header of the request.
   - For versions newer than 13.1.3, the attacker modifies the Host header to "localhost" and includes the hardcoded scheduler secret in the Authorization header.

3) *Gaining Unauthorized Access*
   - The malicious request is sent to the FileWave MDM web server.
   - The web server processes the request, and due to the vulnerability, it fails to properly authenticate the request.
   - The attacker is granted super_user access without needing valid user credentials.

4) *Exploiting the System*
   - With super_user access, the attacker can now perform any action that a legitimate administrator could.
   - The attacker queries the MDM server for a list of all managed devices, extracting sensitive information such as device serial numbers, user emails, locations, etc.
   - The attacker uses the MDM's legitimate functionalities to push malicious packages or commands to the managed devices.

5) *Executing Malicious Actions*
   - The attacker installs malicious software on the managed devices, such as spyware or ransomware.
   - Alternatively, the attacker could modify device configurations, disable security settings, or perform other harmful actions.