PRODUCT SECURITY ADVISORY

UPDATE: September 6, 2024

PSIRT Record Number
CARR-PSA-012-0623

Overview

MAS Monitoring MASmobile Classic (end-of-life March 2022) contains an Authorization Bypass vulnerability (CWE-639) by session ID prediction which allows remote attackers to retrieve sensitive data including customer data, security system status, and event history. The login session is identified by a numeric ID which can be decremented or incremented by the attacker to access data unrelated to the current login.

UPDATE

Additional analysis of the MASmobile Session ID vulnerability has identified an Incorrect Authorization vulnerability in the authorization layer of the MASmobile Classic Services module (CWE-863). As a result, an attacker can use brute force to retrieve the event history of any customer, including all customers. The recommended actions in the Solution section of this advisory also apply to this vulnerability.

MAS Products Impacted	MASmobile Classic and Services (ASP.Net)
Mobile Platforms Impacted	Android, iOS
App Versions Impacted	v1.16.18 and earlier (Android)
MAS ASP.Net Services Versions Impacted	v1.9 and earlier

PSIR Statement

MASmobile Classic was deprecated officially as of March 2022. The MASmobile Classic apps and services were replaced by what is referred to now as “MASmobile”. The impacted apps have not been available in Google Play or the Apple App Store since March 31, 2022. Organizations with active MASmobile Classic and MASmobile Classic

 environments should promptly shut them down and use the new product and services that are not subject to this vulnerability.

https://www.masmonitoring.com/products/web-and-mobile/masmobile

Solution

Since MASmobile and MASmobile Classic and their respective services are different products, MASmobile Classic and MASmobile Classic Services must be uninstalled to eliminate the vulnerability. The affected products are MASmobile Classic app v1.x.x and MASmobile Classic Services v1.7, v1.8, and v1.9. App and service replacement is required.

Note: In some cases, the MASmobile Classic Services may be installed within an IIS MASweb web application. It is not necessary to uninstall MASweb, rather just remove the MASmobile Classic Services.

1. Uninstall MASmobile Classic Services - These services are installed and configured manually in IIS within a virtual directory. To uninstall, unpublish the services in IIS and remove the service files. All versions (v1.7, 1.8, and 1.9) were discontinued.

2. Remove the MASmobile Classic app from Android and iOS devices. All versions (v1.x.x) were discontinued and no longer available in the app stores (Play and AppStore).

3. Contact MAS to arrange the installation of MASterMind EX Services (v6.46 or later). These services do not run under IIS and must be configured in coordination with the customer.

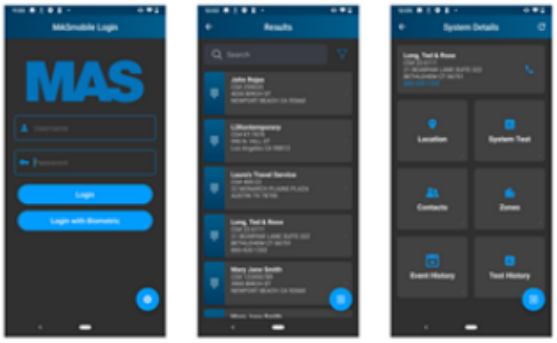
4. Install MASmobile app from Play or AppStore (v2.x.x). This is not an upgrade to MASmobile Classic; it is a different app

Web Version | Update preferences | Unsubscribe Forward

announcement from MAS

To our Valued Customers,

New MASmobile App



We are excited to announce our new MASmobile app for **iOS** and **Android**. The new mobile app has been designed from the ground up with a beautiful new look and feel presenting users with an intuitive experience. Central Station personnel and dealers can view customer data, place systems on or off test, and view system information quickly and easily. The new app supports light and dark mode, and features security enhancements including support for biometric authentication. The new app requires MASterMind version 6.46.01 or higher and MASterMind EX Services.

MASmobile Classic App - End of Life Announcement

With the release of our new MASmobile App, we are formally announcing End-of-Life (EOL) for the MASmobile Classic App. The support for this product will end on March 31st, 2022. After this date no support will be provided for this product and the mobile app will be no longer available for download from the iOS and Android app store. To ensure minimal disruption we recommend customers upgrade to the new MASmobile App.

More information on the new MASmobile app can be found on the **MAS website**. Please contact your Sales or Customer Service representative for assistance.

About Carrier Global Product Cybersecurity

At Carrier, system and operational security is integral. To ensure outcomes, research and development teams leverage Global Product Cybersecurity – a team of highly experienced and credentialed veterans, diverse and dynamic cybersecurity domain experts who've maintained prominent roles and responsibilities in designing, building, and operating highly secure complex systems.

The Product Security Incident Response Team (PSIRT) focuses on the identification, assessment, and disposition of the risks associated with security vulnerabilities within Carrier products, offerings, solutions, components and/or services. PSIRT is a dedicated team of first responders responsible to deliver advanced support designed to contain and minimize the spread and impact of a product security event, incident, breach, and/or crises.

For more information about Global Product Security and PSIRT, please visit us as: https://www.corporate.carrier.com/product-security/

Or you may contact us at: productsecurity@carrier.com

Initial Publication Date	Last Published Date
June 15, 2023	September 6, 2024