Product Security Bulletin

Honeywell

MASmobile Classic Authorization Bypass Vulnerability

Security Bulletin #: 2023-MAS-012-0323

Publish Date: 06-15-2023

CVSS v3.0 Base Score: 6.5 Medium

Reference: CVE-2023-36483

Summary

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.

Attention: Due to the wide variety of security controls, implementations and interfaces, it is the responsibility of each customer to assess the potential impact within a specific operating environment.

Vulnerability Overview

1. MASmobile Classic Authorization Bypass

   CVSS Base Score: 6.5 (Medium)

   CVSS Vector
   http://www.first.org/cvss/calculator/3.0#CVSS:3.0/[vector].

Affected Products

MAS Products Impacted	MASmobile Classic and Services (ASP.Net)
Mobile Platforms Impacted	Android, iOS
App Versions Impacted	v1.16.18 and earlier (Android) v1.7.24 and earlier (iOS)
MASmobile ASP.Net Services Versions Impacted	v1.9 and earlier

Mitigating Factors

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

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

Resolution Description

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.

Acknowledgment

Thanks to Joris Talma, independent .NET developer from The Netherlands, for reporting this potential vulnerability.

Appendix: About CVSS

The Common Vulnerability Scoring System (CVSS) is an open standard for communicating the characteristics and severity of software vulnerabilities. The Base score represents the intrinsic qualities of a vulnerability. The Temporal score reflects the characteristics of a vulnerability that change over time. The Environmental score is an additional score that can be used by CVSS, but is not supplied as it will differ for each customer.

The Base score has a value ranging from 0 to 10. The Temporal score has the same range and is a modification of the Base score due to current temporary factors.

The severity of the score can be summarized as follows:

Severity Rating	CVSS Score
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.

Detailed information about CVSS can be found at http://www.first.org/cvss.

DISCLAIMERS

- CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY.
- YOUR USE OF THE INFORMATION ON THIS DOCUMENT OR MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK.
- HONEYWELL RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME AND WITHOUT NOTICE.
- HONEYWELL PROVIDES THE CVSS SCORES “AS IS” WITHOUT WARRANTY OF ANY KIND. HONEYWELL DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PURPOSE AND MAKES NO EXPRESS WARRANTIES EXCEPT AS MAY BE STATED IN A WRITTEN AGREEMENT WITH AND FOR ITS CUSTOMERS
- IN NO EVENT WILL HONEYWELL BE LIABLE TO ANYONE FOR ANY DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES.