AR2019007

# Prima Systems FlexAir 2.3.38 Multiple Vulnerabilities

**Author: Gjoko Krstic**

**Release Date: May 10, 2019**

# Copyright Notices

## COPYRIGHT NOTICE

## OVERVIEW

Multiple vulnerabilities were found in the Prima Systems FlexAir Access Control Platform. These findings include Default Credentials, Insufficient Session-ID Length, Authentication With MD5 Hash, Predictable Database Name Download, Command Injection, Cross-Site Request Forgery, Stored Cross-Site Scripting, Hard-coded Credentials and Authenticated Script Upload Code Execution.

## AFFECTED PRODUCTS

Prima FlexAir;

The following versions are affected:

- 2.3.38 and bellow

The vulnerabilities have been discovered and validated in Prima FlexAir 2.3.38. Older versions are affected too.

## IMPACT

An unauthenticated user can have full system access.

## BACKGROUND

Prima is an innovative high security brand of access control with certified Security Grade 4. Access control, booking, info-screens, elevator and alarm integration and much more in one operational system. FlexAir® is an access control system build to provide flexibility, high quality and high security.

## VULNERABILITY DETAILS

### Default Credentials

Attackers can easily obtain default passwords and identify Internet-connected target systems. Passwords can be found in product documentation and compiled lists available on the Internet. It is possible to identify exposed systems using search engines like Shodan, and it is feasible to scan the entire IPv4 internet.

Applied Risk has calculated a CVSSv3 score of 9.8 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.

### Command Injection

The application constructs an OS command using externally-influenced input from an upstream component, but incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component. This could allow attackers to execute unexpected, dangerous commands directly on the operating system.

Applied Risk has calculated a CVSSv3 score of 10.0 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H.

### Unrestricted File Upload

The vulnerability exists due to absence of validation of file extensions when uploading files through the Python script upload. A remote and authenticated attacker can upload python applications into directory within application's web root and execute them with privileges of the web server.

Applied Risk has calculated a CVSSv3 score of 9.1 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H.

### Cross-Site Request Forgery

The affected application allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests within index.swf. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site.

Applied Risk has calculated a CVSSv3 score of 5.0 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L.

### Insufficient Session-ID Length

The vulnerability exists due to insufficient value length of Session-ID HTTP header. Once a user is authenticated, the application generates 7 or 8 (depending on the version) digits for the session value. The Session-ID HTTP header can be brute-forced by remote attackers to obtain a valid session and bypass authentication.

Applied Risk has calculated a CVSSv3 score of 4.3 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N.

### Cross-Site Scripting

The application suffers from a stored XSS vulnerability. The issue occurs when input passed via several parameters to several scripts is not sanitized before returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in context of an affected site.

Applied Risk has calculated a CVSSv3 score of 5.4 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N.

### Predictable Database Name Download

The application generates database backup files with a predictable name. A malicious actor can exploit this issue to download the database file and disclose login information that can allow her to bypass authentication and have full access to the system.

Applied Risk has calculated a CVSSv3 score of 9.1 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N.

### Authentication With MD5 Hash

The application allows improper authentication with the MD5 hash value of the password. An attacker can exploit this issue and authenticate to the application without knowing the password of a specific username if previously obtained the database with all the MD5 hash passwords.

Applied Risk has calculated a CVSSv3 score of 8.1 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H.

### Hard-coded Credentials

The application is vulnerable to hard-coded credentials. For the Flash version of the web interface of the application, the username and password are hard-coded within the SWF file that can aid an attacker to easily disclose that information and successfully authenticate.

Applied Risk has calculated a CVSSv3 score of 9.8 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H.

### Authenticated Script Upload Code Execution

The application allows the upload of arbitrary Python scripts when configuring the main central controller. These scripts can be immediately executed with highest privileges allowing an authenticated attacker to gain full system access.

Applied Risk has calculated a CVSSv3 score of 9.1 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H.

## MITIGATION

Prima Systems is aware of the reported vulnerabilities and has released new versions to fix these issues.

## REFERENCES

Vendor website

https://www.primasystems.eu/

Product page

https://primasystems.eu/flexair-access-control/

Common Vulnerability Exposure (CVE):

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7280
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7281
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7666
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7667
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7668
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7669
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7670
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7671
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7672
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9189

## CONTACT DETAILS

For any questions related to this report, please contact Applied Risk Research team at:

Email: research@applied-risk.com

PGP Public Key:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQENBFOgiBQBCACj+Notofe/liuHuc90yy8GAfFn8YFCsMCo7wQmQRNTT43bZQq2
gQr7FTLtOl6rBkOLm8bDk0YY/CtWsjdLh1jlDrWyfU6yIzfcu4CSpn1+5n1ivNN5
17ri+VtmgF392twiKhy2+MC9O4of+GMyu1hy5pIjwi3qGzdNlAnT7m7U/hNzaIR4
ae7+NuWtEvWWKyp3IEEMKTDV/ZOtRD1tfIR8KeBB7Axa8cJdlotw/Ail9TLVB6kt
a/BlvhM/zgWfbEPadnx6B0u7pdW50bTECAs0VHje8mcheTwTCAJo+de3/DqUA34X
oF9aAZWpZWE7VH0O4Q8ZtfrXPFqR2xF8LHhZABEBAAG0REFwcGxpZWQgUmlzayBS
ZXNlYXJjaCBUZWFtIChubyBwYXNzd29yZCkgPHJlc2VhcmNoQGFwcGxpZWQtcmlz
ay5jb20+iQE+BBMBAgAoBQJToIgUAhsjBQkJZgGABgsJCAcDAgYVCAIJCgsEFgID
AQIeAQIXgAAKCRA6nyA79MpeSay8CACSI4UhAget5Z+qEDmz1fe+9krgmx7wwDnF
ig4AVICU8ppJQoUCB5pP6eIV/DM7i+mu8e9zeGlA82t69yTVIANWx72zPmGn5Ku8
4t79gR8V+99PW+O+1rej+96wfL2v+IuOXOcJkTsheUyQZ8Klwc1U8kTdGZEY+/IZ
c32ZhyJ04/cchVP/Zsj2WQIh84wbqa27bTEyyFBnD8FdQ2R4UDTqwACbLgp82m29
P346s80c15RZIX8wUAu0LcNbWJJHRsX6Sa+MozTNug9yWdpZt+nmHEMl95lJYktR
w3+gwyaXeUxALX8Baq2EJDdNx9OlsryiNFdnE9vKIM0+24fTDoqguQENBFOgiBQB
CACtSAm5oBD4kJJY+rtHh6xoytOzP6bFEnrVjqXrXCj+ECG6+N6Droqd072X5hki
qoL1viI4NV+2jrYTtMIu+/nc4zuUFUDRYSm0X/K3WgsqaLA4jdedTm45Tau/Fn6W
26tB5AaddcoDdx6JVGIxFvwU+41KoZ7ouDZo7UEBZ7getPubyR4aPepUsjYnPOUL
0SHH76+b/pC5AZm4crpqWf7Q+qaYQdBIhJbgm5ijFzCyHusYgVGBT1hak81QGpM0
1K9wXki/fJrRyEsWWUjpVSEPRizsFJ60v+NrX50gvvXed8MlX0O9efwgeCmGIVDL
oxF/AmnznYWy0LYWAhh/dW7dABEBAAGJASUEGAECAA8FAlOgiBQCGwwFCQlmAYAA
CgkQOp8gO/TKXkmgdQf/ZtwhL2bs+mlmTUmlT3XO4ekVPRLQKtBYfr8y4rdfnq7Y
MdFYEJAt45R+e4I3I7cIJM1/ImncjFng1EpwFItAXVLa1ktiO6BqT6wBqL6pSBe3
2x5VP8OEnnRubCgYaTotNfiEErgh8cG92tW/TiQArU2dnBcVwYHVwPm450pEv9Aq
BBzgeZ25I1Cv0vlQkQLy9PuTA6DWoxeIxbaMD8ZpKGi+XDrfguJ3tERQMlUA6Fc+
OBkT/NKz8mgecVrwCWbCmScyEhh6onTkevI+mydvsxYG8rE6YVxl3oK5Xi6tvAt9
cUPKKK363nkA1AEoMvTz1bCbmTGvTNWLifoMNtNnGA==
=pAvd
-----END PGP PUBLIC KEY BLOCK-----
```