### Cryptnetix

# Snapt Aria 12.8 Vulnerability Disclosure

It appears your browser does not support HTML5. No biggie... you can <u>click</u> here to download the PDF file.

#### Mitre Reference:

#### CVE-2022-24235

Vulnerability Type: Cross Site Request Forgery (CSRF)

Affected Product Code Base: Snapt Aria - 12.8

Affected Component: Snapt Aria management portal

**Description:** A Cross-Site Request Forgery (CSRF) in the management portal of Snapt Aria v12.8 allows attackers to escalate privileges and execute arbitrary code via unspecified vectors.

**Attack Vectors:** An authenticated user must click on a malicious link which hosts the CSRF payload.

Attack Type: Remote

Impact Code execution: true

Impact Escalation of Privileges: true
Impact Information Disclosure: true

## CVE-2022-24236

Vulnerability Type: Insecure Permissions

Affected Product Code Base: Snapt Aria - 12.8

**Affected Component:** Snapt Aria management portal, email configuration **Description:** An insecure permissions vulnerability in Snapt Aria v12.8 allows unauthenticated attackers to send e-mails from spoofed users' accounts.

Attack Vectors: Exploitation occurs through a maliciously crafted "Test

Email" request, utilizing an unprivileged authentication token.

CVE Impact Other: Impersonation

Attack Type: Remote

### Cryptnetix

#### CVE-2022-24237

VulnerabilityType Other: Authenticated Command Injection

Affected Product Code Base: Snapt Aria - 12.8

Affected Component: Snapt Aria management portal, default snaptPowered2

component

**Description:** The snaptPowered2 component of Snapt Aria v12.8 was discovered to contain a command injection vulnerability. This vulnerability allows authenticated attackers to execute arbitrary commands.

Attack Vectors: Exploitation occurs though command injection of

snaptPowered2 configuration requests.

Attack Type: Remote

Impact Code execution: true

Impact Escalation of Privileges: true
Impact Information Disclosure: true

# Timeline:

01/28/22 - initial contact disclosure

01/31/22 - vendor initial response

**02/07/22** - vendor patch (CVE-2022-24237, CVE-2022-24236, CVE-2022-24235)

02/24/22 - vendor last contact

© 2022 Copyright: <a href="mailto:cryptnetix.com">cryptnetix.com</a>