

Vendor Detailed Report for Release Management

This report provides the results of our assessment on Jan 10, 2023 and is intended to provide an overview of Release Management's cybersecurity risk.

Issued by
Carpe Data

Date
Jan 10, 2023

Vendor Detailed Report for
Release Management

This report has been generated using [UpGuard](#). If you have any questions, please contact support@upguard.com.

Introduction

Carpe Data created this report on Release Management on Jan 10, 2023 based on the following assets: automated scanning of 27 domains & IPs.

These assets are created and stored on the UpGuard platform. UpGuard is a complete third-party risk and attack surface management platform that combines security ratings, security questionnaires, and risk assessments to provide a complete overview of a company's security posture.

The results are summarized into a security rating, a numeric score for cybersecurity performance. Security ratings make it easy to compare organizations and assess performance over time.

To assist with remediation, the report unpacks the security rating into six underlying categories: questionnaire, website security, network security, brand & reputation risk, email security, and phishing & malware. Each category then outlines individual risks, domains & IPs impacted, and provides remediation recommendations. The most severe risks in each category appear first.

To improve Release Management's security rating, focus on questionnaire, website security, and network security risks first, followed by brand & reputation risks, email security, and phishing & malware risks.

If you'd like to see how UpGuard can protect Release Management, [book a demo](#).


How are UpGuard's security ratings calculated?

UpGuard assesses the security posture of millions of organizations every day. We use threat signals gathered from trusted commercial, open-source, and proprietary sources, alongside risks identified in security questionnaires and risk assessments conducted on the UpGuard platform. The hundreds of threat signals we monitor include:

- ✓ Susceptibility to man-in-the-middle attacks
- ✓ Insecure SSL/TLS certificates
- ✓ SPF, DKIM and DMARC settings
- ✓ HTTP Strict Transport Security (HSTS)
- ✓ Email spoofing and phishing risk
- ✓ Vulnerabilities
- ✓ Malware susceptibility
- ✓ Open admin, database, and file sharing ports
- ✓ Exposure to known data breaches and data leaks
- ✓ Secure cookie configuration
- ✓ Results of intelligent security questionnaires

Our ability to combine real-time signals with traditional risk management techniques means we can provide in-depth insights into external and internal security postures. Cybersecurity is a domain where small improvements can make a big difference, we've hired the world's best security experts so our customers don't have to.

Our security ratings range from A-F:

- 
- A** 801-950
Organization has a robust security posture and good attack surface management.
 - B** 601-800
Organization has basic security controls in place but could have large gaps in their security posture.
 - C** 401-600
Organization has poor security controls and has serious issues that need to be addressed.
 - D** 201-400
Organization has severe security issues and should not process any sensitive data.
 - F** 0-200
Organization has not invested in basic security controls and should not be used.

Assessment summary



You are viewing an exported Risk Summary Report for Release Management. To view the full report, or to generate an updated report, please log into the UpGuard Platform.

[View on UpGuard →](#)

This assessment is based on the analysis of Release Management's externally observable security posture as at Jan 10, 2023. Each risk has commentary on why it is a threat and our recommendation for remediation.

Overall cyber risk rating

Overall risk rating

A 914 / 950

This is the overall security rating and is derived from the results of automated scanning. Release Management has a robust security posture and good attack surface management.





Security rating over 12 months

— Your rating - - - Industry average

































Risks identified

Total risks

Critical risks	 0	Critical risks or vulnerabilities that place the business at immediate risk of data breaches.
High risks	 3	Severe risks that should be addressed immediately to protect the business.
Medium risks	 8	Unnecessary security risks that can lead to more serious vulnerabilities.
Low risks	 4	Areas of improvement to reduce risk and improve the businesses' cyber security rating.

Risk breakdown by category

 Website security	 914	 0	 0	 8	 3
 Email security	 950	 0	 0	 0	 0
 Network security	 932	 0	 3	 0	 1
 Phishing & malware	 950	 0	 0	 0	 0
 Brand & reputation risk	 950	 0	 0	 0	 0

Risk details

Website security

Website security identifies potential attack vectors like vulnerabilities, cross-site scripting, susceptibility to man-in-the-middle attacks, and other exploits. Any successful exploit can impact business, customers, and regulatory compliance.

Overall risk rating

A **914** / 950

Critical risks

 0

High risks

 0

Medium risks

 8

Low risks

 3



Website security risk breakdown

 **HTTP Strict Transport Security (HSTS) not enforced** 2 domains & IPs with this risk

Issue

Websites are not enforcing HTTP Strict Transport Security (HSTS). Without enforcing HSTS, visitors are susceptible to certain man-in-the-middle attacks.

Recommendation

Configure the website to enforce HSTS by setting up the Strict-Transport-Security header, which ensures browsers will only communicate over HTTPS.

Domains & IPs

Expected

Actual

159.69.211.7

[header set]

[not set]

162.55.157.194

[header set]

[not set]

Website security risk breakdown (continued)

!! Insecure SSL/TLS versions available 1 domain/IP with this risk

Issue

Impacted websites are using an insecure SSL/TLS version. Any version of the SSL protocol, and TLS protocol prior to version 1.2 are now insecure. Websites should not use these protocols.

Recommendation

Disable support of the SSL protocol and TLS protocol prior to version 1.2. Doing so will ensure the integrity of communications between the website and its visitors.

Domains & IPs	Expected	Actual
releasemanagement.app	[none found]	TLSv1, TLSv1.1

!! SSL expires within 20 days 1 domain/IP with this risk

Issue

Impacted domains have SSL certificates which are set to expire within 20 days. When certificates expire they become invalid, and will no longer be able to run secure transactions.

Recommendation

We recommend that you renew impacted SSL certificates prior to their expiry to avoid unencrypted communications. This helps keep your customers safe by ensuring adequate encryption.

Domains & IPs	Expected	Actual
ci.releasemanagement.app	[does not expire in the next 20 days]	2023-01-22 14:02:24 UTC

Website security risk breakdown (continued)

Secure cookies not used

3 domains & IPs with this risk

Issue

When secure cookies are not used, there is an increased risk of third-parties intercepting information contained in those cookies. Cookies are widely used because they allow websites to store data directly on the user's browser, such as their session.

Recommendation

Configure the websites so all cookies have the Secure attribute set. This limits the scope of the cookie to secure channels, meaning they will only be transmitted over HTTP.

Domains & IPs	Expected	Actual
162.55.157.194	<code>[all set-cookie headers include 'secure']</code>	<code>Set-Cookie: JSESSIONID HttpOnly;</code>
167.235.105.23	<code>[all set-cookie headers include 'secure']</code>	<code>Set-Cookie: JSESSIONID HttpOnly;; Set-Cookie: atlassian.xsrf.token</code>
demo.releasemanagement.app	<code>[all set-cookie headers include 'secure']</code>	<code>Set-Cookie: JSESSIONID HttpOnly;; Set-Cookie: atlassian.xsrf.token</code>

Server information header exposed

1 domain/IP with this risk

Issue


The web server information of the impacted websites is exposed. Exposing information about the server version increases the ability of attackers to exploit known vulnerabilities.

Recommendation

Configure these websites to prevent version information from being revealed by removing the 'Server' header. This reduces the chance of attackers successfully exploiting known vulnerabilities.

Domains & IPs	Expected	Actual
ci.releasemanagement.app	<code>[does not contain version number]</code>	<code>nginx/1.18.0 (Ubuntu)</code>

Website security risk breakdown (continued)

 **X-Frame-Options is not deny or sameorigin (Provisional)** 8 domains & IPs with this risk

Issue

Impacted domains allow browsers to display their content in frames. This can lead to clickjacking attacks.

Recommendation

The website needs to set the X-Frame-Options header to deny or sameorigin. Alternatively, configure a Content Security Policy with the frame-ancestors directive. This will prevent browsers from displaying the website's content in frames.

Domains & IPs	Expected	Actual
162.55.152.233	[deny or sameorigin]	[not set]
162.55.158.66	[deny or sameorigin]	[not set]
49.12.16.55	[deny or sameorigin]	[not set]
release-gadgets.releasemanagement.app	[deny or sameorigin]	[not set]
rmcloud-prd.releasemanagement.app	[deny or sameorigin]	[not set]
rmcloud-stg.releasemanagement.app	[deny or sameorigin]	[not set]
uboard-stg.releasemanagement.app	[deny or sameorigin]	[not set]
uboard.releasemanagement.app	[deny or sameorigin]	[not set]

Website security risk breakdown (continued)

!! CSP implemented unsafely (Provisional) 3 domains & IPs with this risk

Issue

Impacted domains do not have a Content Security Policy implemented safely. This increases the risk of XSS attacks.

Recommendation

The Content Security Policy for this website should use a nonce or hash with 'unsafe-inline' and restrict appropriate sources.

Domains & IPs	Expected	Actual
162.55.157.194	[implemented safely]	frame-ancestors 'self'
167.235.105.23	[implemented safely]	frame-ancestors 'self'
demo.releasemanagement.app	[implemented safely]	frame-ancestors 'self'

!! CSP is not implemented (Provisional) 1 domain/IP with this risk

Issue

Impacted domains do not have a valid Content Security Policy implemented. This increases the risk of XSS and clickjacking attacks.

Recommendation

A Content Security Policy for this website should be designed and implemented.

Domains & IPs	Expected	Actual
159.69.211.7	[valid policy]	[not set]

! HSTS header does not contain includeSubDomains 1 domain/IP with this risk

Issue

The HTTP Strict Transport Security (HSTS) header on identified websites does not contain the includeSubDomains directive. Without this directive, the browser won't enforce the HSTS policy over subdomains.

Recommendation

Include the includeSubDomains directive. This ensures the HSTS policy is applied to the website and all subdomains, preventing them from accepting connections through HTTP.

Domains & IPs	Expected	Actual
167.235.105.23	max-age=[anything]; includeSubDomains; ...	max-age=31536000

Website security risk breakdown (continued)

 **CSP contains unsafe-eval (Provisional)** 1 domain/IP with this risk

Issue


Impacted domains allow unsafe-eval in their Content Security Policy, reducing protection against XSS attacks.

Recommendation

The Content Security Policy for this website should use not allow unsafe-eval.

Domains & IPs	Expected	Actual
releasemanagement.app	[no unsafe-eval]	base-uri 'self';object-src 'none';report-uri /_/view/cspreport;script-src 'nonce-7OGwnzPkmK50vWXwn1OwHw' 'unsafe-inline' 'unsafe-eval';worker-src 'self';frame-ancestors https://google-admin.corp.google.com/

Website security risk breakdown (continued)

 X-Content-Type-Options is not nosniff (Provisional)

9 domains & IPs with this risk

Issue

Impacted domains are not preventing MIME sniffing by setting the X-Content-Type-Options header to nosniff. This can lead to MIME confusion attacks.

Recommendation

The website needs to set the X-Content-Type-Options header to nosniff. This will prevent browsers from interpreting files as a different MIME type than what is specified in the Content-Type HTTP Header.

Domains & IPs	Expected	Actual
159.69.211.7	<code>nosniff</code>	<code>[not set]</code>
162.55.152.233	<code>nosniff</code>	<code>[not set]</code>
162.55.158.66	<code>nosniff</code>	<code>[not set]</code>
49.12.16.55	<code>nosniff</code>	<code>[not set]</code>
release-gadgets.releasemanagement.app	<code>nosniff</code>	<code>[not set]</code>
rmcloud-prd.releasemanagement.app	<code>nosniff</code>	<code>[not set]</code>
rmcloud-stg.releasemanagement.app	<code>nosniff</code>	<code>[not set]</code>
uboard-stg.releasemanagement.app	<code>nosniff</code>	<code>[not set]</code>
uboard.releasemanagement.app	<code>nosniff</code>	<code>[not set]</code>

Website security risk breakdown (continued)

i CAA not enabled

8 domains & IPs with this risk

Issue

The domain does not contain a valid CAA record.

Recommendation

Where possible, specify the Certificate Authorities that are authorized to issue certificates for this domain in a CAA DNS record.

Domains & IPs	Expected	Actual
ci.releasemanagement.app	[set]	[not set]
demo.releasemanagement.app	[set]	[not set]
release-gadgets.releasemanagement.app	[set]	[not set]
releasemanagement.app	[set]	[not set]
rmcloud-prd.releasemanagement.app	[set]	[not set]
rmcloud-stg.releasemanagement.app	[set]	[not set]
uboard-stg.releasemanagement.app	[set]	[not set]
uboard.releasemanagement.app	[set]	[not set]

i Atlassian Jira 8.22.1 has potential vulnerabilities

1 domain/IP with this risk

Issue

Atlassian Jira 8.22.1 has known vulnerabilities published in the Common Vulnerabilities and Exposures (CVE) database. In some situations, these vulnerabilities can be exploited.

Recommendation

Check affected domains to determine whether the vulnerabilities are present and if so, apply the required patch or work around to fix security issues.

Domains & IPs	Expected	Actual
demo.releasemanagement.app	[none found]	CVE-2022-26135, CVE-2022-26136, CVE-2022-26137

Website security risk breakdown (continued)

i NGINX 1.18.0 has potential vulnerabilities 1 domain/IP with this risk

Issue

NGINX 1.18.0 has known vulnerabilities published in the Common Vulnerabilities and Exposures (CVE) database. In some situations, these vulnerabilities can be exploited.

Recommendation

Check affected domains to determine whether the vulnerabilities are present and if so, apply the required patch or work around to fix security issues.

Domains & IPs	Expected	Actual
ci.releasemanagement.app	[none found]	CVE-2021-3618, CVE-2021-23017, CVE-2022-3638, CVE-2022-41741, CVE-2022-41742

i Unmaintained page detected 1 domain/IP with this risk

Issue

This domain appears to be unmaintained based on indicators like page content or status code. Unmaintained pages expand the attack surface for malicious actors.

Recommendation

Review the page and decommission it if it is not active or maintained.

Domains & IPs	Expected	Actual
167.235.111.224	[not detected]	Status Code: 503

Email security

Email security is an important part of enterprise risk management. Email is a popular medium for spreading malware and conducting social engineering attacks. Inadequate email security makes it easy for attackers to send malicious email on a domain's behalf, increasing the efficacy of phishing and other business email compromise attacks.

Overall risk rating

A **950** / 950

Critical risks

 0

High risks

 0

Medium risks

 0

Low risks

 0



Email security risk breakdown

No risks detected in this category.

Network security

Network security identifies externally-facing, insecure network settings that can enable man-in-the-middle attacks, and aid in the spread of self-replicating computer worms such as WannaCry. These worms exploit known vulnerabilities in the services that run behind open ports to spread. By fixing network issues, there is reduced risk of successful exploitation and spread.

Overall risk rating

A 932 / 950

Critical risks

!!!! 0

High risks

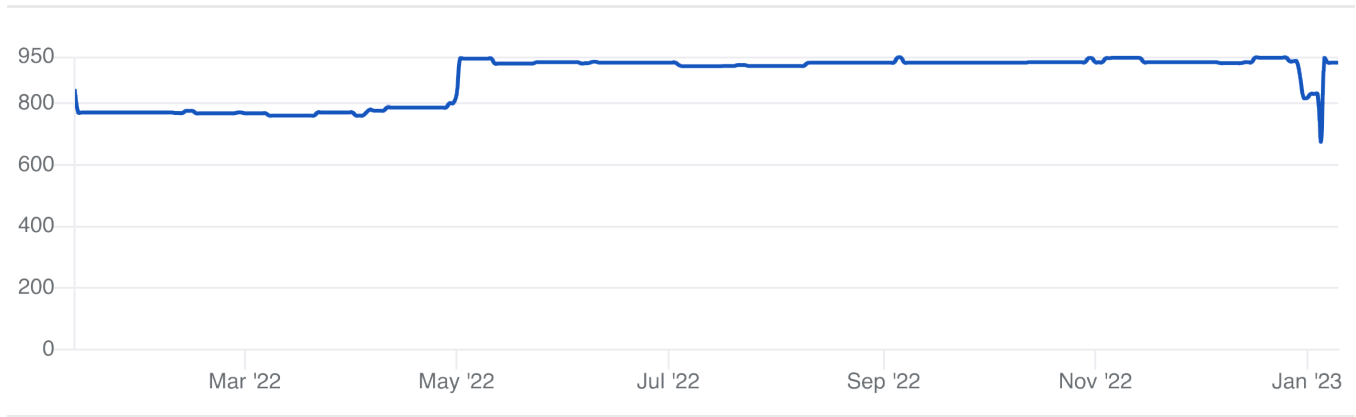
!!! 3

Medium risks

!! 0

Low risks

! 1



Network security risk breakdown

!!! 'portmapper' port open

1 domain/IP with this risk

Issue

We've detected that the 'portmapper' port is open.

Recommendation

We recommend that the 'portmapper' port be closed to reduce the attack surface.

Domains & IPs

Expected

Actual

releasemanagement.app

[closed]

```
'portmapper': [listening on port 111]
```

Network security risk breakdown (continued)

!!! Potentially vulnerable to CVE-2022-26136 (Atlassian Arbitrary Servlet Filter Bypass) 1 domain/IP with this risk

Issue

The vulnerability in self-hosted Atlassian products allows a remote, unauthenticated attacker to bypass authentication used by third party apps.

Recommendation

The Atlassian product instance should be upgraded to the latest available patch version as soon as possible.

Domains & IPs

Expected

Actual

demo.releasemanagement.app

[not vulnerable]

[potentially vulnerable]

!!! Potentially vulnerable to CVE-2022-26137 (Atlassian Additional Servlet Filter Invocation) 1 domain/IP with this risk

Issue

The vulnerability in self-hosted Atlassian products allows attackers to access the vulnerable application with a victim's permissions using a CORS bypass attack.

Recommendation

The Atlassian product instance should be upgraded to the latest available patch version as soon as possible.

Domains & IPs

Expected

Actual

demo.releasemanagement.app

[not vulnerable]

[potentially vulnerable]

! DNSSEC not enabled 1 domain/IP with this risk

Issue

We've detected that DNSSEC is missing from some domains. DNSSEC provides DNS resolvers origin authentication of DNS data, authenticated denial of existence and data integrity but not availability or confidentiality.

Recommendation

The domain owner should turn on DNSSEC for all domains. This can generally be done at their domain name registrar.

Domains & IPs

Expected

Actual

releasemanagement.app

true

false

Network security risk breakdown (continued)

i 'HTTP' port open 1 domain/IP with this risk

Issue

We've detected that the 'HTTP' port is open.

Recommendation

We recommend that the 'HTTP' port be closed to reduce the attack surface.

Domains & IPs

Expected

Actual

ci.releasemanagement.app

[closed]

'HTTP': [listening on port 8081]

Phishing & malware

Phishing & malware outlines websites that are suspected of hosting malware, unwanted software, or phishing pages. Left unchecked these pages damage your brand, infect customers, and lead to costly data breaches.

Overall risk rating

A **950** / 950

Critical risks

 0

High risks

 0

Medium risks

 0

Low risks

 0



Phishing & malware risk breakdown

No risks detected in this category.

Brand & reputation risk

Brand protection highlights situations where a domain could be hijacked, expired, or deleted at the domain name registrar or domain name registry. By fixing these issues, there is a reduced risk of domains being tampered with via social engineering and other cyber attacks.

Overall risk rating

 **950** / 950

Critical risks

 0

High risks

 0

Medium risks

 0

Low risks

 0



Brand & reputation risk risk breakdown

No risks detected in this category.

Vendor Information

Primary domain

releasemanagement.app

Evidence used to generate this report

Automated scanning

This report includes analysis performed on the following vendor domains & IPs on Jan 10, 2023. If risk assessments are included, automated scanning is based on the last assessment date. Otherwise results are based on the latest available data.

Active domains & IPs

15

Inactive domains

12

Total domains & IPs scanned

27



Only the active domains & IPs are shown in this report.

releasemanagement.app

7 subdomains

159.69.211.7

0 subdomains

162.55.152.233

0 subdomains

162.55.157.194

0 subdomains

162.55.158.66

0 subdomains

167.235.105.23

0 subdomains

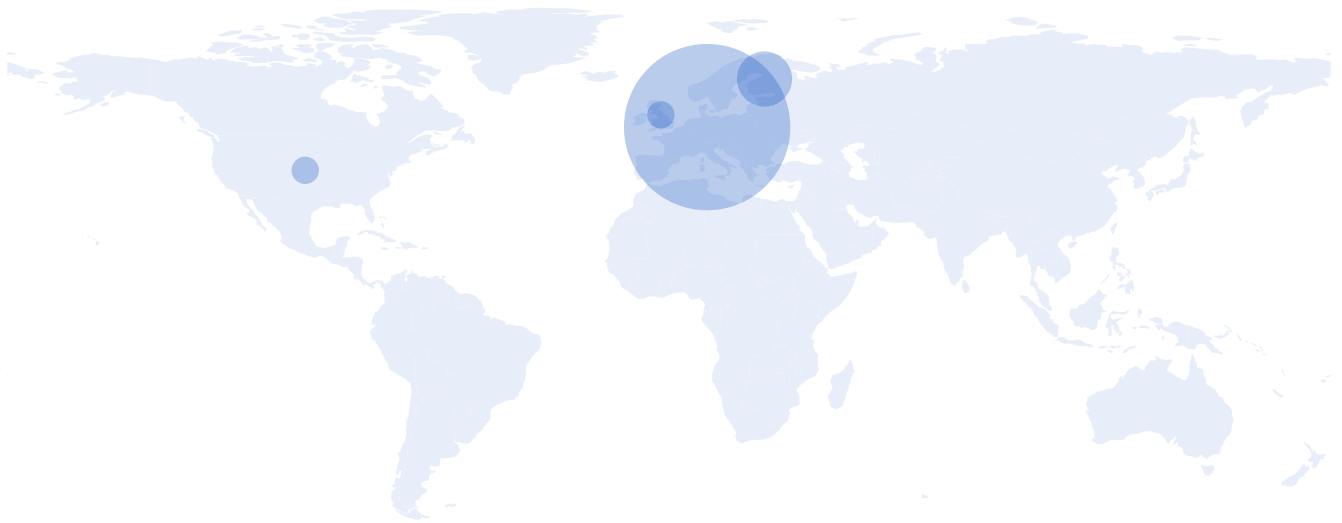
167.235.111.224

0 subdomains

49.12.16.55

0 subdomains

Geolocation risk



Geolocation risk breakdown

This report includes analysis performed on IP addresses spread across the following countries.

Hosting countries

4

IP addresses

16



Germany

11 IP addresses

69%



Finland

3 IP addresses

19%



United Kingdom

1 IP address

6%



United States

1 IP address

6%