Hewlett Packard
Enterprise

HPE Security
Fortify Runtime

Software Version: 17.3
Versions 2017.1.3 (Java) and 2017.1.3 (.NET)

Application Protection Rulepack Kit Guide

Document Release Date: April 2017
Software Release Date: April 2017

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise Development products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The software is restricted to use solely for the purpose of scanning software for security vulnerabilities that is (i) owned by you; (ii) for which you have a valid license to use; or (iii) with the explicit consent of the owner of the software to be scanned, and may not be used for any other purpose.

You shall not install or use the software on any third party or shared (hosted) server without explicit consent from the third party.

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.protect724.hpe.com/community/fortify/fortify-product-documentation

You will receive updated or new editions if you subscribe to the appropriate product support service. Contact your HPE sales representative for details.

Contents

Preface

Contacting HPE Security Fortify Support

If you have questions or comments about using this product, contact HPE Security Fortify Technical Support using one of the following options.

To Manage Your Support Cases, Acquire Licenses, and Manage Your Account

https://support.fortify.com

To Email Support

fortifytechsupport@hpe.com

To Call Support

1.844.260.7219

For More Information

For more information about HPE Security software products: http://www.hpe.com/software/fortify

About the Documentation Set

The HPE Security Fortify Software documentation set contains installation, user, and deployment guides for all HPE Security Fortify Software products and components. In addition, you will find technical notes and release notes that describe new features, known issues, and last-minute updates. You can access the latest versions of these documents from the following HPE Security user community website:

https://www.protect724.hpe.com/community/fortify/fortify-product-documentation

You will need to register for an account.

Change Log

The following table lists changes made to this document. Revisions to this document are published only if the changes made affect product functionality.

Software Release / Document Version	Changes
17.3	Added: • Malformed Request: Bad Content-Type • Slow Method Call: Slow Database Query (Batch Processing) • Slow Method Call: Slow Database Query (Web Processing)
16.8	Minor updates.
16.6	Added: • LDAP Injection • OGNL Expression Injection: Direct Method Invocation

Chapter 1: Rule Categories for Rulepacks

The information in this section describes the detection capabilities of Fortify RTAP Rulepacks. Specifically, for each category of attack, vulnerability, or audit event detected by RTAP, HPE Security provides the following information.

Programming Language

Many RTAP rules often apply across multiple programming languages, but in cases where a rule applies only to one language or another we indicate so here.

Event Type

RTAP rules produce three types of events: attack, vulnerability, and audit. Rules that identify malicious activity produce attack events. Rules that identify vulnerabilities in the program definition produce vulnerability events. Rules that report information intended to help audit or debug the behavior of the program produce audit events. Many rules produce events that span multiple types, such as SQL injection, which produces events that represent an attack, vulnerability, and an activity relevant to an auditor all at the same time.

Priority

Events have one of four priorities associated with them: critical, high, medium, and low. Critical-priority events represent the most serious problems and low-priority events the least.

Default Response

A solid understanding of default behavior, as well as of any customization deemed necessary, is critical to a successful RTAP deployment. Rules can use the following actions, all of which are included in the default configuration:

- *ignore*—take no action (still logs event)
- *display404/display403*—respond with a 404 or 403 error
- *rewrite*—transform data per rule-specific instructions

Detection Strategy

The detection strategy implemented by a rule describes the combination of program and data characteristics that cause the rule to trigger and produce an event.

Configuration

Many rules have externalized configuration values that can be modified to fine-tune the behavior of the rule. The configuration template associated with a program protected by RTAP defines the configuration values, as described in the topics for those particular rules. To modify these values through HPE Security Fortify Software Security Center, view the details for the configuration template you wish to modify and navigate to the template-defined variables section.

Tuning

While Fortify Runtime and the RTAP rule set are designed to work well on most programs with little or no intervention, some categories of detection benefit from targeted testing, verification, and tuning. In these cases, you might want to adjust the configuration to accommodate changes that are warranted.

Chapter 2: HPE Security Fortify Application Protection Rules

This section contains the following topics:

ClassLoader Manipulation: Struts

Language	Event Type	Priority	Default Response
Java	Attack, Vulnerability, Audit	High	Default Action

Detection Strategy

Triggers when the property resolver is trying to access the classloader. The following frameworks are supported:

- Struts version 1, via monitoring Apache commons-beanutils
- Struts version 2, via monitoring OGNL APIs

Non-vulnerable versions will not be triggered.

Supported Frameworks

Java	.NET
Apache Struts version 1 Apache Struts version 2	n/a

Configuration

None

Tuning

None

Command Injection

Language	Event Type	Priority	Default Response
Java, .NET	Attack, Vulnerability, Audit	High	Default Action

Detection Strategy

Matches any system command execution that contains a cross-boundary HTTP request parameter OR where the command contains more than one command (for example, a one-line batch command with "&&" or "|").

According to command line grammar, a "boundary" is a position between two lexical tokens. For example, the boundaries for "`ping -n 4 localhost`" are "`ping|-n|4|localhost`" and a string value "`ping -n`" is therefore a cross-boundary input while "localhost" is not.

Supported Frameworks

Java	.NET
Core Java	Core .NET

Configuration

None

Tuning

None

Command Injection: Shellshock

Language	Event Type	Priority	Default Response
Java	Attack, Vulnerability, Audit	High	Default Action

Detection Strategy

Triggers if any HTTP header value starts with "() {"

Supported Frameworks

Java	.NET
Core Java	n/a

Configuration

None

Tuning

None

Cookie Security: HTTPOnly Not Set on Session Cookie

Language	Event Type	Priority	Default Response
Java	Vulnerability, Audit	Medium	Rewrite

Detection Strategy

This rule works as a virtual patch on application servers, as listed in the following table, that either do not support the HttpOnly cookie flag or do not enable the flag on HTTP Session cookie by default.

Type	Supports HttpOnly Session Cookie Since	Comment
Apache Tomcat	5.5.28[1] or 6.0.20	Default "false" for 5.5.28 to 6.0. Default "true" for 7.0 and later.
Red Hat JBoss[2]	6.0	Servlet 3.0, default "false," config via web.xml <cookie-config>
Oracle WebLogic	9.2 MP4[3]	Servlet 2.4, default "true"
IBM WebSphere[4]	8.0[5]	Servlet 3.0, default "true," configurable in console

For all servers, the rule installs the virtual patch only if it is operating in Protect mode. HPE Security Fortify Application Defender sends events for this rule only during server startup.

[1] http://tomcat.apache.org/tomcat-5.5-doc/config/context.html

[2] According to https://www.owasp.org/index.php/HTTPOnly, JBoss 5.1 supports HttpOnly by using `Context.xml` (similar to Tomcat 5.5).

[3] http://download.oracle.com/docs/cd/E13222_01/wls/docs92/webapp/weblogic_xml.html#wp1071982

[4] http://www-01.ibm.com/support/docview.wss?uid=swg1PK80629, the custom property `addHttpOnlyAttributeToCookies` on WAS 6.1 and 7.0 does not affect every cookie that passes through the application server. The list of non-HTTPOnly cookies includes `JSESSIONID` cookies.

[5] http://publib.boulder.ibm.com/infocenter/ieduasst/v1r1m0/index.jsp?topic=/com.ibm.iea.was_v8/was/8.0/Security/ WASv8_SecurityEnhancements/player.html

On Apache Tomcat and Red Hat JBoss servers, one event is triggered and the virtual patch is installed for each application context during the context startup. After a context startup, disabling this rule or changing it from Protect mode to Monitor mode has no further effect (that is, the virtual patch remains installed and the HttpOnly flag remains enabled).

On Oracle WebLogic and IBM WebSphere servers, only one event is triggered during the entire application server startup. After server startup, disabling this rule or changing it from Protect mode to Monitor mode prevents the addition of the HttpOnly flag on subsequent HTTP sessions.

Supported Frameworks

Java	.NET
Apache Tomcat Red Hat Jboss Oracle WebLogic IBM WebSphere	n/a

Configuration

None

Tuning

Disable this rule if your application uses JavaScript to access the session cookie.

Cross-Site Scripting Attack

Language	Event Type	Priority	Default Response
Java, .NET	Attack, Vulnerability, Audit	Critical	Default Action

Detection Strategy

Matches HTTP request parameter names and values that contain values associated with cross-site scripting attacks (the request values may be HTML decoded and stripped of white space prior to matching).

Potential attack strings include the introduction of relevant tags, such as `<script/>` and `<link/>`, as well as a variety of JavaScript functions.

Supported Frameworks

Java	.NET
Servlet API	System.Web

Configuration

The Default Action (`default_action`) option controls the default response for events that are not explicitly handled in another way. Default configurations set this value to *display*, which will cause RTAP to display a default HTML error page. This behavior should be customized for production deployments.

Tuning

Test that suspected cross-site scripting strings are not expected in normal request traffic. When suspected cross-site scripting strings appear in normal request traffic, you should suppress the event accordingly. see *Appendix* for more information about tuning and specific detection capabilities of the RTAP Rulepack.

Dangerous File Inclusion: Local

Language	Event Type	Priority	Default Response
Java, .NET	Attack, Vulnerability, Audit	High	Default Action

Detection Strategy

Triggers when the application server is trying to include a local file in the HTTP response, if there is an HTTP request parameter that a) contains the base file name of the file to be included and b) also meets **any** of the following conditions:

- It contains both ".." and "/"
- It starts with "file:"
- It is equal to the full path of the file to be included
- It matches the internal HPE Security blacklist.

Supported Frameworks

Java	.NET
Core Java	System.Web

Configuration

None

Tuning

None

Dangerous File Inclusion: Remote

Language	Event Type	Priority	Default Response
Java, .NET	Attack, Vulnerability, Audit	High	Default Action

Detection Strategy

Triggers when the application server is trying to include a remote file in the HTTP response, if **all** of the following conditions are met:

- The URL host for the remote file to be included is not identical to the HTTP request host header.
- There is an HTTP request parameter that contains the full URL.
- The HTTP request parameter does not match the RfiWhiteList regular expression pattern (see below).

Supported Frameworks

Java	.NET
Core Java	Core .NET

Configuration

RfiWhiteList is a white list regular expression pattern for Dangerous File Include: Remote. Each entry in the list should include a full URL (including a protocol such as http://). If a URL exactly matches an entry, or if a URL matches an entry and the URL also includes a substring after the match, that URL is allowed and will **not** trigger an event. The pattern is case insensitive.

Example list entry: ^http[s]?://www.mydomain.com/public/

Tuning

None

Denial of Service: Parse Double

Language	Event Type	Priority	Default Response
Java	Attack, Vulnerability, Audit	High	Rewrite

Detection Strategy

Matches calls to the method `readJavaFormatString` in class `FloatingDecimal` and `FormattedFloatingDecimal`.

This rule will only be executed in the following known vulnerable Java versions:

- JRE 1.6.0_23 or earlier
- JRE 1.5.0_27 or earlier
- JRE 1.4.2_29 or earlier

Supported Frameworks

Java	.NET
Core Java	n/a

Configuration

None

Tuning

None

Directory Listing

Language	Event Type	Priority	Default Response
Java	Attack, Vulnerability, Audit	High	Display 403

Detection Strategy

Matches calls to methods that list the contents of a server-side directory.

Supported Frameworks

Java	.NET
Core Java	n/a

Configuration

None

Tuning

Test that the program does not intentionally list the contents of any local directories.

Some application servers will not return a 403 error if the server is configured to prevent Directory Listing. If this is the case, you may want to create a custom event handler that changes the default response to a different response code to diminish the risk of information leakage.

Discovery: Known Vulnerability Scanner Activity

Language	Event Type	Priority	Default Response
Java, .NET	Attack	Critical	Default Action

Detection Strategy

Matches HTTP request “User-Agent” header and other headers against the list of known scanner names.

Supported Frameworks

Java	.NET
Servlet API	System.Web

Configuration

Name	Description	Default Value
AllowedScannerIPs	HTTP request with known Vulnerability Scanner is blocked unless it is from AllowedScannerIPs. The value is a regular expression and is matched against the remote IP address (not host name).	127\.0\.0\.1

Tuning

None

Dynamic Code Evaluation: Unsafe Deserialization

Language	Event Type	Priority	Default Response
Java	Attack, Vulnerability, Audit	Critical	Throw Exception

Detection Strategy

Monitor object deserialization process and report event if:

1. A deserialized object is, implements, or extends from any black-listed Java classes.
2. The deserialization method requires any of the following Java security permission
   - FilePermission – except read
   - SocketPermission – except resolve
   - PropertyPermission – except read

Supported Frameworks

Java	.NET
Core Java	n/a

Configuration

None

Tuning

None

Forceful Browsing

Language	Event Type	Priority	Default Response
Java, .NET	Attack, Audit	Medium	Display 404

Detection Strategy

Matches requests for resources that include resources names commonly targeted by attackers, including `.log`, `.bak`, `.old`, `_log`, `_bak`, and `_old`.

Supported Frameworks

Java	.NET
Servlet API	System.Web

Configuration

Forceful browsing events will, by default, cause RTAP to send a 404 error. Before using RTAP to protect against forceful browsing, ensure that you have an appropriate custom error page configured in your application or application server. Then, set the Display Default Forward URL under System Defined settings to instruct RTAP to forward to the appropriate URL for the error page.

Note: IIS must be specifically configured to send requests for the extensions matched by this rule on to applications, otherwise RTAP does not witness them and cannot protect against forceful browsing.

Tuning

Test that the program does not intentionally provide access to any resources with these extensions.

Header Manipulation

Language	Event Type	Priority	Default Response
Java, .NET	Attack, Vulnerability, Audit	High	Rewrite

Detection Strategy

When adding or modifying the HTTP header name:

- The string cannot contain any characters ranging from 0x00 to 0x19 inclusive.
- The string cannot start with a space (`'\s'`) or tab (`'\t'`)
- The string cannot contain a colon ':'
- The application server is vulnerable to HTTP Response Splitting

When adding or setting the HTTP header value:

- The string cannot contain '\r' or '\n'.
- The application server is vulnerable to HTTP Response Splitting

Note: The following Fortify Runtime supported application servers are found to be vulnerable to HTTP Response Splitting

Application Server	Vulnerable Version
IBM WebSphere	All
Oracle WebLogic	All

Note: Both WebSphere and WebLogic throw an exception if '\r' or \n' is injected into HTTP header. However, they both allow the injection if '\r' or '\n' is followed by a space or a tab which means line continuation according to RFC. On the other hand, since Internet Explorer (tested version: 6/8/11) completely ignores the line continuation syntax, these application servers have to be considered as vulnerable.

Supported Frameworks

Java	.NET
Apache Tomcat Red Hat Jboss	System.Web

Java	.NET
Oracle WebLogic IBM WebSphere	

Configuration

Name	Description	Default Value
`ProtectHmOnAllAppServers`	Most application servers are not vulnerable to Header Manipulation attacks. By default, all attacks are logged but the protection action is only applied if it is running on a vulnerable application server. Set the `<ProtectHmOnAllAppServers>` value to true to force protection action even when the application server is not vulnerable.	False

Tuning

None

LDAP Injection

Language	Event Type	Priority	Default Response
Java, .NET	Attack, Vulnerability, Audit	Critical	Throw

Detection Strategy

An event is triggered if the LDAP search filter contains either

- An invalid syntax, such as unbalanced parenthesis or a dangling search term.
- A cross-boundary HTTP request parameter.

According to LDAP grammar, a "boundary" is a position between two lexical tokens. For example, the boundaries for "(&(name=John Doe)(l=San Francisco))" are "(|&|(|name|=|John Doe|)|(|l|=|San Francisco|)|)" and a string value "John Doe)(l=" is therefore a cross-boundary input while "John" is not.

Supported Frameworks

Java	.NET
javax.naming.directory	System.DirectoryServices

Configuration

None

Tuning

None

Malformed Request: Bad Content-Type

Language	Event Type	Priority	Default Response
Java	Attack	High	Default Action

Detection Strategy

The rule triggers if the HTTP Content-Type contains either '%{' or '${' which is the attack signature for Apache Struts2 S2-045 vulnerability. Please visit https://struts.apache.org/docs/s2-045.html for detail information about the vulnerability.

Supported Frameworks

Java	.NET
Servlet API	n/a

Configuration

None

Tuning

None

Malformed Request: Missing Accept Header

Language	Event Type	Priority	Default Response
Java, .NET	Attack	Low	Default Action

Detection Strategy

The received HTTP Request does not contain an Accept header.

Supported Frameworks

Java	.NET
Servlet API	System.Web

Configuration

None

Tuning

None

Malformed Request: Missing Content-Type

Language	Event Type	Priority	Default Response
Java, .NET	Attack	Low	Default Action

Detection Strategy

HTTP Request without Content-Type when Content-Length is larger than zero.

Supported Frameworks

Java	.NET
Servlet API	System.Web

Configuration

None

Tuning

None

Malformed Request: Use of Unsupported Method

Language	Event Type	Priority	Default Response
Java	Attack	Low	Default Action

Detection Strategy

Matches the HTTP request method against a configurable list.

Supported Frameworks

Java	.NET
Servlet API	n/a

Configuration

Name	Description	Default Value
AllowedHttpMethods	HTTP request methods not listed in here is blocked. This value is a case sensitive regular expression. Example: GET|POST|PUT	GET|POST|PUT

Tuning

None

Method Call Failure: Database Query

Language	Event Type	Priority	Default Response
Java, .NET	Audit	Low	Ignore

Detection Strategy

Triggers when SQL exceptions are thrown upon database query execution.

Supported Frameworks

Java	.NET
JDBC Hibernate 2 Hibernate 3/4/5 JPA JDO	Core .NET

Configuration

None

Tuning

Create event handlers to discard events for exceptions that do not represent program failures.

OGNL Expression Injection: Direct Method Invocation

Language	Event Type	Priority	Default Response
Java	Attack, Vulnerability	Critical	Default Action

Detection Strategy

If Struts2 Direct Method Invocation (DMI) is enabled and:

- The method name contains forbidden characters such as '[', ']', '(', ')', or
- The method name equals "getClass", "toString" or "wait"

This rule is related to a known vulnerability, S2-032, in Apache Struts 2.x. The rule is NOT triggered if DMI is not enabled or if the application is using a well-patched, non-vulnerable version of Struts2.

Supported Frameworks

Java	.NET
Apache Struts version 2	N/A

Configuration

None

Tuning

None

Open Redirect

Language	Event Type	Priority	Default Response
Java, .NET	Attack, Vulnerability, Audit	High	Default Action

Detection Strategy

Report when HTTP 302 is triggered and/or a “Location” header field is added to the HTTP response with the following conditions:

- The location is not a relative path.
- The host part of the location is not “localhost”, or “127.0.0.1”.
- The host part of the location is not the same as indicated in the HTTP Request “Host” header, if any.
- The host part of the location is not a sub-domain of the HTTP Request "Host" header, if any.

Supported Frameworks

Java	.NET
Servlet API	System.Web

Configuration

None

Tuning

To allow redirect to a different URL, add the following event handler to `rt_config.xml`.

```
<EventHandler description="Allowing the following URL from Open Redirect"
              label="OpenRedirectException" propagate="false" >
   <Match>
      <MatchAttribute name="category">Open Redirect</MatchAttribute>
      <MatchAttribute name="Trigger">www.example.com</MatchAttribute>
   </Match>
   <Handle/>
</EventHandler>
```

Poor Error Handling: Unhandled Exception

Language	Event Type	Priority	Default Response
Java, .NET	Vulnerability, Audit	High	Default Action

Detection Strategy

Triggers when unhandled exceptions reach the top-level application server context.

Supported Frameworks

Java	.NET
Servlet API	System.Web

Configuration

The Default Action (`default_action`) option controls the default response for events that are not explicitly handled in another way. Default configurations set this value to *display*, which will cause RTAP to display a default HTML error page. This behavior should be customized for production deployments.

Tuning

None

Privacy Violation: Internal

Language	Event Type	Priority	Default Response
Java, .NET	Vulnerability, Audit	High	Rewrite (mask)

Detection Strategy

Matches when plain text and unmasked credit card numbers or Social Security numbers are being written to internal systems such as log files.

Supported Frameworks

Java	.NET
Apache Commons Logging (JCL) java.util.logging (JUL) Log4j javax.servlet.GenericServlet.log() Simple Logging Facade for Java (Slf4j)	Microsoft Enterprise Logging Library Log4Net Nlog Response.AppendToLog()

Configuration

None

Tuning

Slow Method Call: Slow Database Query (Batch Processing)

Language	Event Type	Priority	Default Response
Java, .NET	Audit	Low	Ignore

Detection Strategy

Triggers when a database connection takes longer than a given threshold (default 10,000 milliseconds) to establish.

Note: This is a monitor only rule because the rule will not stop a running query even though it runs over time.

Supported Frameworks

Java	.NET
JDBC	ADO.NET

Configuration

Name	Description	Default Value
SQLTimeThreshold	ADO.NET	3000

Tuning

Test under load to ensure that normal operating parameters do not exceed the threshold.

Slow Method Call: Slow Database Query (Web Processing)

Language	Event Type	Priority	Default Response
Java, .NET	Audit	Low	Ignore

Detection Strategy

Triggers when a database connection takes longer than a given threshold (default 10,000 milliseconds) to establish.

Note: This is a monitor only rule because the rule will not stop a running query even though it runs over time.

Supported Frameworks

Java	.NET
JDBC	ADO.NET

Configuration

Name	Description	Default Value
WebSQLTimeThreshold	Default database query time threshold used to generate Slow Method Call: Slow Database Query (Web Request) events. Measured in milliseconds.	10000

Tuning

Test under load to ensure that normal operating parameters do not exceed the threshold.

SQL Injection

Language	Event Type	Priority	Default Response
Java, .NET	Attack, Vulnerability, Audit	Critical / Low	Ignore Outside of Request Scope / Ignore

Detection Strategy

1. The full SQL string, with string literals normalized to 'a' and numbers normalized to 0 and comments removed, matches any predefined signatures (note, line command "--" and block comment "/*" themselves are signatures, but can be excluded).
2. The full SQL string contains a cross-boundary HTTP request parameter.

A "boundary" is a position between two lexical tokens according to SQL grammar. For example, the boundaries for "select * from users where name = 'john' and 1=1" are "select|*|from|users|where|name|=|'john'|and|1|=|1" and a string value "john' and 1=1" is therefore a cross-boundary input while "john" is not.

Attack strings are divided into a high-accuracy group with a Critical priority and a Default Action response inside a request scope, and a low-accuracy group with a Low priority and an Ignore response.

Supported Frameworks

Java	.NET
JDBC	ADO.NET
Hibernate version 2	NHiberate
Hibernate version 3/4/5	Entity Framework version 4/5/6
JPA	
JDO	

Configuration

None

Tuning

Some applications and frameworks incorrectly add "or 1=1" to SQL queries. In these cases, RTAP will erroneously block legitimate requests. If this happens, you should suppress the event accordingly.

see*Appendix* or more information about tuning and specific detection capabilities of the RTAP Rulepack.

System Information Leak

Language	Event Type	Priority	Default Response
Java	Vulnerability, Audit	High	Ignore

Detection Strategy

Triggers when exception stack traces are printed directly to the HTTP response.

Supported Frameworks

Java	.NET
Core Java	System.Web

Configuration

None

Tuning

None

XML Entity Expansion Injection

Language	Event Type	Priority	Default Response
Java, .NET	Attack, Vulnerability, Audit	High	throw

Detection Strategy

Triggers when the XML parser is expanding a general or parameter entity and the resolved length is longer than a specific value.

The following XML parsers are supported:

- Apache Xerces v1, v2 (including Xerces embedded in JRE 5+)
- Woodstox XML processor
- .NET built-in XML parser

Supported Frameworks

Java	.NET
Xerces version 1 Xerces version 2 Woodstox version 4	System.Xml

Configuration

Name	Description	Default Value
MaxEntityExpansionLength	Maximum allowed string length for XML Entity Expansion. Entity expansion that exceeds this value will trigger an XML Entity Expansion Injection Event.	50000

Tuning

None

XML External Entity Injection

Language	Event Type	Priority	Default Response
Java, .NET	Attack, Vulnerability, Audit	High	throw

Detection Strategy

Triggers when the XML parser is resolving an external general or parameter entity.

The following XML parsers are supported:

- Apache Xerces v1, v2 (including Xerces embedded in JRE 5+)
- Woodstox XML processor
- .NET built-in XML parser

Supported Frameworks

Java	.NET
Xerces version 1 Xerces version 2 Woodstox version 4	System.Xml

Configuration

None

Tuning

None

XPath Injection

Language	Event Type	Priority	Default Response
Java, .NET	Attack, Vulnerability, Audit	Critical	Default Action

Detection Strategy

The XPath string contains a cross-boundary HTTP request parameter.

A “boundary” is a position between two lexical tokens according to XPath grammar. For example, the boundaries for “//Employee[UserName/text()='blah' or 'a'='a' And Password/text()='blah']” are “//|Employee|[|UserName|text|()=|’john’|or|’a’|=|’a’|And|Password|/text|()=|’1234’|]” and a string value “john’ or ‘a’=’a” is therefore a cross-boundary input while “john” is not.

Supported Frameworks

Java	.NET
javax.xml JDom version 1 JDom version 2	System.Xml.XPath

Configuration

None

Tuning

None

Appendix : Eliminating Hard-Coded XSS and SQLi Issues

Note: This appendix applies to the detection capabilities and tuning of the RTAP Rulepack only.

SQL queries that contain hardcoded statements like 1=1 will by default be blocked by RTAP. This is unwanted behavior, and RTAP should be tuned accordingly. Until recently, it was only possible to disable the rule entirely.

A similar XSS issue can be addressed with this technique. For example, a database can contain HTML tags by default. RTAP recognizes this as an attack by default.

With this feature, there is no need to disable the rule entirely. Instead, only a portion of the rule has to be disabled (that is, a particular monitor). The particular monitor has to be disabled by inserting a new `Eventhandler` in the configuration file. Afterward, a new custom rule (which is a tuned version of the disabled one) must be inserted to diminish exposure.

For this scenario, assume that 1=1 is hardcoded in a SQL query. For example, the application contains the following statement:

```
String query= "SELECT * FROM db WHERE 1=1";
```

When the above code is executed, the following RTAP event triggers by default:

```
[2010-06-17T10:27:31.140+0200 EVENT]
SQL Injection
{
       timestamp: 1276763251140
       category: SQL Injection
       suggestedAction: ignoreActionWithoutRequest
       kingdom: Input Validation and Representation
       description: /java/sql_injection.htm?version=2010.3.0.0002
       eventType: attack,vulnerability,audit
       impactBias: integrity
       audience: medium,targeted,broad,dev
       primaryAudience: security
       coveredSCA: yes
       priority: Critical
       RuleID: a05dfa1c-0cd3-4a4b-9c26-f3d852b6f09f
       MonitorID: 3552E9D5-83EA-4A1D-8361-68518AEF9D77
       location: at
```

```
org.apache.tomcat.dbcp.dbcp.PoolingDataSource$PoolGuardConnectionWrapper.p
repareStatement(PoolingDataSource.java) \
       ...
```

As this is normal application code, we do not want to block this query. By adding the following `EventHandler` in the `EventHandlers` in the configuration file (`rt_config.xml`), RTAP can be tuned so that it does not block this query. Events generated by the monitor `3552E9D5-83EA-4A1D-8361-68518AEF9D77` is ignored instead of blocked (by default).

```
<EventHandler description="Drop events with a suggested action of
'ignore'" label="Ignore action">
        <Match>
           <MatchAttribute name="MonitorID">3552E9D5-83EA-4A1D-8361-
68518AEF9D77</MatchAttribute>
        </Match>
        <!-- no dispatch.  these events die here. -->
</EventHandler>
```

Doing this creates a security vulnerability in the RTAP protected application, because adding this `EventHandler` will switch off a very small portion of the protection. Of course, actions must be taken to make the security vulnerability as small as possible. In most cases, it is possible to keep the vulnerability nonexistent.

Reducing security risk can be done by, first, reintroducing the monitor (in a new, similar rule). The new rule should exclude only the very specific statement. For example, when 1=1 is in the query by default, we can reintroduce the following rule:

```
<Rule>
       <RuleID>DD6F1044-B938-4782-9D2A-6655886981C3</RuleID>
    <ProgramPoints>
        <SetReference id="DatabaseQueries"/>
    </ProgramPoints>
    <Monitors>
        <ExtensionSpec base="SQLi" monitorID="7DCAB8FD-1679-4153-836E-
        165085D04DEE">
            <Predicate>
                InvalidSql(Input) or
                (
                    ParseSql(Input) contains part :
                  { not part matches 1=1 and part matches /(?i)
                  (^|[\s\(]\d+(\.\d*)?)\s*
(=|!=|&lt;=|&gt;=|&lt;|&gt;|&lt;&gt;|
                  (not\s*)?between)\s*($|\d+(\.\d*)?|N)/ }
```

```
                )
            </Predicate>
        </ExtensionSpec>
    </Monitors>
</Rule>
```

Here, RTAP will protect the application against injection strings like 2=2, or 3=3, but not against 1=1.

To reduce the risk further, HPE recommends that you replace any “always true” statements (of the form `1=1`) with a true statement that is hard to guess (or random); for example: `19810107=19810107`. This way, a brute force attack on the system will generate a significant number of issues and can be used to lock out the user before it can find the accepted true statement. The rule should be changed as follows:

```
<Rule>
    <RuleID>DD6F1044-B938-4782-9D2A-6655886981C3</RuleID>
    <ProgramPoints>
        <SetReference id="DatabaseQueries"/>
    </ProgramPoints>
    <Monitors>
        <ExtensionSpec base="SQLi" monitorID="7DCAB8FD-1679-4153-836E-
        165085D04DEE">
            <Predicate>
                InvalidSql(Input) or
                (
                    ParseSql(Input) contains part :
                  { not part matches 19810107=19810107 and part matches /(?i)
                  (^|[\s\(]\d+(\.\d*)?)\s*
(=|!=|&lt;=|&gt;=|&lt;|&gt;|&lt;&gt;|
                  (not\s*)?between)\s*($|\d+(\.\d*)?|N)/ }
                )
            </Predicate>
        </ExtensionSpec>
    </Monitors>
</Rule>
```

A third action you should take is to switch off the monitor for the very specific location (which is a stack trace). A custom event handler must be created to disable SQL Injection protection for the specific pages where this occurs. The handler should be as specific as possible, so as not to allow potential attacks to go through.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Application Protection Rulepack Kit Guide (HPE Security Fortify Runtime 17.3)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to HPFortifyTechPubs@hpe.com.

We appreciate your feedback!