



ADSelfService Plus

[Email Download Link](#)

Security Advisory

Self Service Password Management » Security Advisory



Free Edition



Quick Links

[Get Quote](#)

[Extend Trial License](#)

[Online Demo](#)

[Request Support](#)

[Compare Edition](#)

[Success Stories](#)

[Pricing & Purchase](#)

[ROI Calculator](#)



[Password Self-Service](#)



[Documents](#)



[Key Topics](#)

Related Products

[ADManager Plus](#)

[ADAudit Plus](#)

[Exchange Reporter Plus](#)

[EventLog Analyzer](#)

[M365 Manager Plus](#)

[DataSecurity Plus](#)

[RecoveryManager Plus](#)

Security advisory - ADSelfService Plus authentication bypass vulnerability

CVE code.: CVE-2021-40539

Severity.: Critical

Versions affected.: ADSelfService Plus builds up to 6113

Fix: [ADSelfService Plus build 6114](#) (Sep 7, 2021)

This page covers details of the vulnerability and an incident response plan if your system is affected. For more information on the latest updates and the timeline of the vulnerability, you can [visit this page](#). Have questions about this vulnerability? Check out [our detailed FAQ page](#). You can also sign up for a complementary vulnerability audit [on this page](#). Our emergency support team will help you through a one-on-one session and manually run the tool, check for indicators of compromise, and answer all your questions.

We have partnered with [Veracode](#), an independent application security company, to conduct manual pen tests on ADSelfService Plus so that we get a third-person perspective on the security footing of the solution.

Introduction

We were notified about an authentication bypass vulnerability in ADSelfService Plus affecting the REST API URLs that could result in remote code execution.

Details

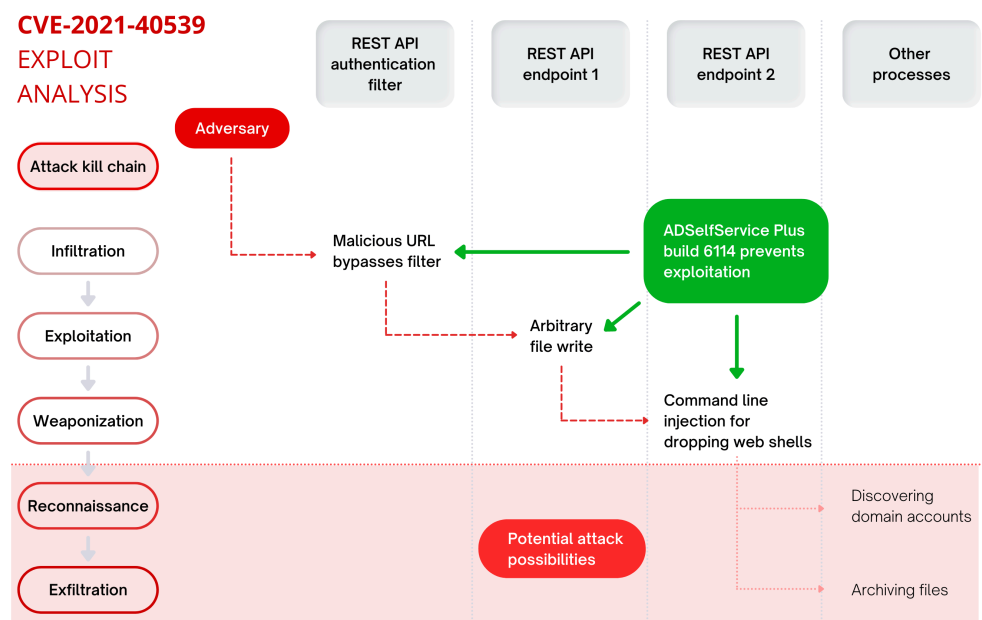
ManageEngine

ADSelfService Plus

[Email Download Link](#)

AD Free Tools

security filter due to an error in normalizing the URLs before validation. This, in turn, gave attackers access to REST API endpoints, and they exploited the endpoints to perform subsequent attacks such as arbitrary command execution. The following exploit analysis flowchart shows how the attackers exploited the vulnerability.



CVE-2021-40539 exploit analysis flowchart

How do I check if my installation is affected?

There are three ways to check if your installation is affected:

- [Run our exploit detection tool.](#)
- [Check for specific log entries.](#)
- [Check for specific files in your system.](#)

1. Run our exploit detection tool

Note: A discrepancy was found while running an earlier version of this tool as an administrator. This was reported by Cyberoo CERT and has been fixed as of June 2, 2023.

Once you have downloaded the file, follow these steps:

- i. Extract the tool to the **\ManageEngine\ADSelfService Plus\bin** folder.
- ii. Right-click on the **RCEScan.bat** file, and select **Run as administrator**.
- iii. A Command Prompt window will open and the tool will run a scan. If your installation is affected, you will get the following message:
"Result: Your ADSelfService Plus installation is affected by authentication bypass vulnerability."

If you want to check for logs manually, you can follow the steps given below.

2. Check for specific log entries

i. Access logs

In the **\ManageEngine\ADSelfService Plus\logs** folder, search the access log files with the pattern **"access_log_<date>.txt"** and check for entries with the strings listed below:

- a. `././RestAPI`
- b. `././RestAPI`

The image below shows an access log entry example with the above mentioned strings:

```
- /ServletApi [././RestAPI/LogonCustomization] "-" 10.59.0.204 10.59.0.204 GET [04/Sep/2021:18:53:44 +0530] 112 136038 404 "TestMace/1.3.3"  
- /test/./RestAPI/LogonCustomization "-" 10.59.8.67 10.59.8.67 POST [17/Sep/2021:19:18:57 +0530] 885 136012 404 "TestMace/1.3.3"  
- [././RestAPI/LogonCustomization] "-" 10.59.8.67 10.59.8.67 POST [17/Sep/2021:19:19:36 +0530] 119 136012 404 "TestMace/1.3.3"  
- [././RestAPI/LogonCustomization] "-" 10.59.8.67 10.59.8.67 POST [17/Sep/2021:19:21:05 +0530] 151 136012 404 "TestMace/1.3.3"
```

ii. ServerOut logs

ManageEngine ADSelfService Plus

[Email Download Link](#)

```
java.lang.NullPointerException: org.apache.catalina.connector.RequestBase cannot be cast to  
com.adventnet.iam.security.SecurityRequestWrapper  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at com.adventnet.sym.adm.common.webclient.util.ClientUtil.getFileFromRequest(ClientUtil.java:768) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at com.adventnet.sym.adm.common.webclient.admin.LogonCustomization.unspecified(LogonCustomization.java:91) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at org.apache.struts.actions.DispatchAction.dispatchMethod(DispatchAction.java:245) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at org.apache.struts.actions.DispatchAction.execute(DispatchAction.java:170) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at org.apache.struts.chain.commands.servlet.ExecuteAction.execute(ExecuteAction.java:58) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at org.apache.struts.chain.commands.AbstractExecuteAction.execute(AbstractExecuteAction.java:67) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at org.apache.struts.chain.commands.ActionCommandBase.execute(ActionCommandBase.java:51) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at org.apache.commons.chain.impl.ChainBase.execute(ChainBase.java:191) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at org.apache.commons.chain.generic.LookupCommand.execute(LookupCommand.java:305) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at org.apache.commons.chain.impl.ChainBase.execute(ChainBase.java:191) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at org.apache.struts.chain.ComposableRequestProcessor.process(ComposableRequestProcessor.java:283) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at org.apache.struts.action.ActionServlet.process(ActionServlet.java:1913) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at org.apache.struts.action.ActionServlet.doPost(ActionServlet.java:462) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at javax.servlet.http.HttpServlet.service(HttpServlet.java:652) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at javax.servlet.http.HttpServlet.service(HttpServlet.java:733) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:231) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at com.manageengine.ads.fw.filter.ADSFilter.doFilter(ADSFilter.java:74) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166) |  
[19:21:04:912] [[09-17-2021]] [SYSERR] [INFO] [40]: at com.manageengine.adssp.server.metrack.NETrackFilter.doFilter(NETrackFilter.java:47) |
```

iii. ADS logs

In the **\ManageEngine\ADSelfService Plus\logs folder**, search the access log files with the pattern "**adslog_<date>.txt**" and check for Java traceback errors that include references to **NullPointerException** in **addSmartCardConfig** or **getSmartCardConfig** as shown in the image below:

```
[19:21:04:915] [[09-17-2021]] [ADSLogger] [INFO] [40]: |  
ava.lang.NullPointerException  
at com.manageengine.ads.fw.authentication.smartcard.SmartCardAPI.addSmartCardConfig(SmartCardAPI.java:423)  
at com.manageengine.ads.fw.authentication.smartcard.SmartCardAction.addSmartCardConfig(SmartCardAction.java:91)  
at com.manageengine.ads.fw.authentication.smartcard.SmartCardAction.addSmartCardConfig(SmartCardAction.java:79)  
at com.adventnet.sym.adm.common.webclient.admin.LogonCustomization.unspecified(LogonCustomization.java:93)  
at org.apache.struts.actions.DispatchAction.dispatchMethod(DispatchAction.java:245)  
at org.apache.struts.actions.DispatchAction.execute(DispatchAction.java:170)  
at org.apache.struts.chain.commands.servlet.ExecuteAction.execute(ExecuteAction.java:58)  
at org.apache.struts.chain.commands.AbstractExecuteAction.execute(AbstractExecuteAction.java:67)  
at org.apache.struts.chain.commands.ActionCommandBase.execute(ActionCommandBase.java:51)  
at org.apache.commons.chain.impl.ChainBase.execute(ChainBase.java:191)  
at org.apache.commons.chain.generic.LookupCommand.execute(LookupCommand.java:305)  
at org.apache.commons.chain.impl.ChainBase.execute(ChainBase.java:191)  
at org.apache.struts.chain.ComposableRequestProcessor.process(ComposableRequestProcessor.java:283)  
at org.apache.struts.action.ActionServlet.process(ActionServlet.java:1913)  
at org.apache.struts.action.ActionServlet.doPost(ActionServlet.java:462)  
at javax.servlet.http.HttpServlet.service(HttpServlet.java:652)  
at javax.servlet.http.HttpServlet.service(HttpServlet.java:733)  
at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:231)  
at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)  
at org.apache.tomcat.websocket.server.WsFilter.doFilter(WsFilter.java:52)  
at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193)  
at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)  
at com.manageengine.ads.fw.filter.ADSFilter.doFilter(ADSFilter.java:74)  
at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:193)  
at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:166)  
at com.manageengine.adssp.server.metrack.NETrackFilter.doFilter(NETrackFilter.java:47)
```

3. Check for specific files in the system

If you are running ADSelfService Plus version 6113 or lower, and if your system has been affected, your system may have the following files in the ADSelfService Plus installation folder:

- i. **service.cer** in the **\ManageEngine\ADSelfService Plus\bin** folder.



ADSelfService Plus

[Email Download Link](#)

- iii. **adap.jsp** in the `\ManageEngine\ADSelfService Plus\webapps\adssp\help\html\promotion` folder.
- iv. **custom.bat** and **custom.txt** files in the `C:\Users\Public\` folder.

Additionally, the below IoCs were published by CrowdStrike on Jun 22, 2023, in connection to their observation of a threat activity suspected to be exploiting CVE-2021-40539.

- v. **selfsdp.jspx** in `\ManageEngine\ADSelfService Plus\webapps\adssp\html\promotion\` folder.
- vi. **error.jsp** in `\ManageEngine\ADSelfService Plus\webapps\adssp\html\` folder.
- vii. **tomcat-ant.jar** in `\ManageEngine\ADSelfService Plus\lib\` folder.
- viii. **Any folder other than selfservice** in `\ManageEngine\ADSelfService Plus\work\Catalina\localhost\ROOT\org\apache\jsp\` folder.

Incident response plan

Check for system compromise:

- Run our exploit detection tool
 - Check for access logs
 - Check for specific files in the system



Is your system compromised?



Yes ↓



ADSelfService Plus

Email Download Link

2. Back up the ADSelfService Plus database using these steps .	2. If you need any difficulties touch with us security@manageengine.com
3. Format the compromised machine. Note: Before formatting the machine, ensure that you have backed up all critical business data.	
4. Download and install ADSelfService Plus. A. The build version of the new installation should be the same as that of the backup. B. It is highly recommended to utilize a different machine for the new installation.	
5. Restore the backup and start the server.	
6. Once the server is up and running, update ADSelfService Plus to the latest build, 6114, using the service pack .	
7. Check for unauthorized access or use of accounts. Also, check for any evidences of lateral movement from the compromised machine to other machines. If there are any indications of compromised Active Directory accounts, initiate password reset for those accounts.	
8. If you need further information, have any questions, or face any difficulties updating ADSelfService Plus, contact our emergency support hotline: adselfserviceplus-security@manageengine.com or +1.408.916.9890 (toll free)	



ADSelfService Plus

[Email Download Link](#)

Need further assistance?

Fill this form, and we'll contact you rightaway.

Name

Business Email *

Phone *

Problem Description *

Country

France



Submit

Reset

☐ Yes, I would like to receive marketing communication regarding [Zoho's](#) products, services, and events from Zoho and its regional partners.

By clicking 'Submit' you agree to processing of personal data according to the [Privacy Policy](#).

Highlights

Password self-service

Free Active Directory users from attending lengthy help desk calls by allowing them to self-service their password resets/ account unlock tasks. Hassle-free password change

ManageEngine

ADSelfService Plus

[Email Download Link](#)

with their Active Directory credentials. Thanks to ADSelfService Plus!

Password/Account Expiry Notification

Intimate Active Directory users of their impending password/account expiry by mailing them these password/account expiry notifications.

Password Policy Enforcer

Ensure strong user passwords that resist various hacking threats with ADSelfService Plus by enforcing Active Directory users to adhere to compliant passwords via displaying password complexity requirements.

Password Synchronizer

Synchronize Windows Active Directory user password/account changes across multiple systems, automatically, including Office 365, G Suite, IBM iSeries and more.

Directory Self-Update & Corporate Search

Portal that lets Active Directory users update their latest information and a quick search facility to scout for information about peers by using search keys, like contact number, of the personality being searched.

[« Home](#)

[Knowledge Base »](#)

ADSelfService Plus trusted by

ManageEngine

ADSelfService Plus

[Email Download Link](#)



Embark on a journey towards identity security and Zero Trust

Password management

Adaptive MFA

Enterprise SSO

Self-service & security

Related products

Self-service password reset

Self-service account unlock

Web-based domain password change

Password expiration notifications

Password synchronization

Password policy enforcer

Cached credentials update

Reporting and auditing

Password self-service from logon screens

Mobile password management

Password security and compliance

Active Directory password audit



Live Demo



Compare Editions



Free Edition



Get Quote



Buy Now

[About us](#) | [EULA](#) | [Terms of service](#) | [Security](#) | [Compliance](#) | [Privacy policy](#) |

[Cookie policy](#) | [Affiliate program](#) | [Newsletter](#) | [Contact sales](#) | [Our offices](#) |

[Global \(English\)](#) ▼

© 2024 Zoho Corporation Pvt. Ltd. All rights reserved.