

ManageEngine ADSelfService Plus privilege escalation - CVE-2021-27214

Friday, 19 February 2021  Horizon Security Staff

ManageEngine ADSelfService Plus

Horizon Security discovered a Server-side request forgery (SSRF) vulnerability in ManageEngine ADSelfService Plus version 6013 and lower which allows an attacker to perform a privilege escalation attack.

If exploited, allows an unauthenticated attacker to send a crafted HTTP request and perform a Cross-site scripting (XSS) stored attack within the administrative portal. From version 6013 to 6000 user interaction is required to trigger the XSS, meanwhile from version 5917 and lower no interaction is needed.

The vulnerability has been fixed by ManageEngine with update 6100.

Discovered by Flavio Baldassi,
Horizon Offensive Security Team

References:

[ManageEngine AdSelfService plus Release Notes](#)
[CVE-2021-27214](#)

Close

We and selected third parties use cookies or similar technologies for technical purposes and, with your consent, for other purposes as specified in the cookie policy. Denying consent may make related features unavailable.

Use the  button to consent to the use of such technologies.

Accept

Scopri di più

ManageEngine ADSelfService Plus privilege escalation - CVE-2021-27214

Friday, 19 February 2021  Horizon Security Staff

ManageEngine ADSelfService Plus

Horizon Security discovered a Server-side request forgery (SSRF) vulnerability in ManageEngine ADSelfService Plus version 6013 and lower which allows an attacker to perform a privilege escalation attack.

If exploited, allows an unauthenticated attacker to send a crafted HTTP request and perform a Cross-site scripting (XSS) stored attack within the administrative portal. From version 6013 to 6000 user interaction is required to trigger the XSS, meanwhile from version 5917 and lower no interaction is needed.

The vulnerability has been fixed by ManageEngine with update 6100.

Discovered by Flavio Baldassi,
Horizon Offensive Security Team

References:

[ManageEngine AdSelfService plus Release Notes](#)
[CVE-2021-27214](#)

We and selected third parties use cookies or similar technologies for technical purposes and, with your consent, for other purposes as specified in the cookie policy. Denying consent may make related features unavailable.

Use the [Accept](#) button to consent to the use of such technologies.

ManageEngine ADSelfService Plus privilege escalation - CVE-2021-27214

Friday, 19 February 2021  Horizon Security Staff

ManageEngine ADSelfService Plus

Horizon Security discovered a Server-side request forgery (SSRF) vulnerability in ManageEngine ADSelfService Plus version 6013 and lower which allows an attacker to perform a privilege escalation attack.

If exploited, allows an unauthenticated attacker to send a crafted HTTP request and perform a Cross-site scripting (XSS) stored attack within the administrative portal. From version 6013 to 6000 user interaction is required to trigger the XSS, meanwhile from version 5917 and lower no interaction is needed.

The vulnerability has been fixed by ManageEngine with update 6100.

Discovered by Flavio Baldassi,
Horizon Offensive Security Team

References:

[ManageEngine AdSelfService plus Release Notes](#)
[CVE-2021-27214](#)

We and selected third parties use cookies or similar technologies for technical purposes and, with your consent, for other purposes as specified in the cookie policy. Denying consent may make related features unavailable.

Use the [Accept](#) button to consent to the use of such technologies.