CVE-2020-13168

SysAid 20.1.11b26 allows reflected XSS via the `ForgotPassword.jsp` `accountid` parameter.

Timeline

- **Discovered:** March 5, 2020
- **Initial Vendor Contact:** March 5, 2020
- **Reported:** May 19, 2020
- **CVE ID issued:** May 19, 2020
- **Secondary Vendor Contact: (Vendor did not reply to initial contact)**: May 28, 2020
- **Public Release:** October 1, 2020

Version Details

Affected Versions:

- 20.1.11b26 and prior

Credit

Will Porter, Lodestone Security (https://www.lodestonesecurity.com/)

References

Public Disclosure

POC Exploit

The following URL path and query parameters will trigger an XSS vulnerability.

```
/ForgotPassword.jsp?accountid=%3C%2Fscript%3E%3Cscript%3Ealert(%27xss%27);var%20a=%27&email=&userName=
```

Circumvention of XSS Protection Setting

During vendor communication I received the following email:

> I will need to forward this SR to our teams to look into this and provide additional details. In the meantime, there is one option referring to cross-site scripting which can be enabled within the SysAid admin portal-> Settings-> customize-> Appearance-> "Modify the "<" character to secure against cross-site scripting".
>
> Please enable it and let me know if the specific .jsp still poses the vulnerabilities.

The `Modify the "<" character to secure against cross-site scripting` did not adequately protect against XSS. While the originally submitted payload was no longer valid, a new payload was trivial to develop.

Modified payload

```
/ForgotPassword.jsp?accountid='+%2B+alert('xss')+%2B+'7&email=&userName=
```

I sent the following email and the vendor did not respond.

> Hi,
>
> This setting appears to be a filter that filters the < character. While enabling this setting prevents the payload that I originally posted from being executed, the filter does not ensure the content is properly encoded and it is possible to exploit using a payload that does not require the < character. To prove the vulnerability still exists I have created a new payload.
>
> /ForgotPassword.jsp?accountid='+%2B+alert('xss')+%2B+'7&email=&userName=

> As you can see this payload does not require the < character, but still executes arbitrary JavaScript. In this sense a filter is insufficient to prevent XSS attacks and it will be necessary to ensure that any user input that is reflected in HTML is properly encoded for the area it is reflected to.
>
> Thanks,
>
> Will Porter
>
> Senior Security Consultant, Exploiter of Vulnerabilities