

eGain Chat 15.5.5 Cross Site Scripting

Authored by [Hassy Vinod Eshan](#), [Brandon Ming Yang Ho](#)

Posted Jul 28, 2021

eGain Chat version 15.5.5 suffers from a cross site scripting vulnerability.

tags | [exploit](#), [xss](#)

advisories | [CVE-2020-15948](#)

SHA-256 | [86f82233af5a41046687330cd64e5466b63f4308ade16bd242d6db2f54261ee8](#) [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

Change Mirror

Download

```
# Exploit Title: eGain Chat 15.5.5 Cross-Site Scripting
# Vendor Homepage: https://www.egain.com/
# Software Link: https://www.egain.com/chat-software/
# Exploit Authors: Brandon Ming Yang Ho (https://www.linkedin.com/in/minhobrandon/), Hassy Vinod Eshan
# CVE: CVE-2020-15948

# Timeline
- June 2020: Initial vulnerability discovery
- July 2020: Reported to eGain Corporation
- August 2020: Fix/patch provided by eGain Corporation
- September 2020: Public disclosure notified to eGain Corporation
- July 2021: Published CVE-2020-15948

# 1. Introduction

eGain Chat is a real time chat assistance solution by eGain Corporation for website visitors to communicate
with chat agents.

# 2. Vulnerability Details

eGain Chat version 15.5.5 is vulnerable to reflected Cross-Site Scripting (Reflected XSS).

The "Name" input field (full_name) does not fully sanitise user input for special characters such as "<" or ">"
and HTML attributes such as "<a href=". It is possible for an attacker to bypass filtering and create malicious
scripts. Once the response has been rendered, the malicious JavaScript code would be executed.

# 3. Proof of Concept

The "Name" input field (full_name) of the chat window can be injected with the following XSS payload as a Proof
of Concept to execute a javascript alert popup.

Payload - <a href="javascript:alert(document.domain)">click/a</a>

# 4. Remediation

Apply the latest fix/patch from eGain Corporation.

# 5. Credits

- Brandon Ming Yang Ho (https://www.linkedin.com/in/minhobrandon/)
- Hassy Vinod Eshan (https://www.linkedin.com/in/hassy-vinod/)
```

[Login](#) or [Register](#) to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: December 2022 <

Su	Mo	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					

Top Authors In Last 30 Days

Red Hat 150 files
Ubuntu 68 files
LiquidWorm 23 files
Debian 16 files
malvuln 11 files
nu11security 11 files
Gentoo 9 files
Google Security Research 6 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older
File Inclusion (4,165)	
File Upload (946)	

File Tags	File Archives
Firewall (821)	December 2022
Info Disclosure (2,660)	November 2022
Intrusion Detection (867)	October 2022
Java (2,899)	September 2022
JavaScript (821)	August 2022
Kernel (6,291)	July 2022
Local (14,201)	June 2022
Magazine (586)	May 2022
Overflow (12,419)	April 2022
Perl (1,418)	March 2022
PHP (5,093)	February 2022
Proof of Concept (2,291)	January 2022
Protocol (3,435)	Older
Python (1,467)	
Remote (30,044)	
Root (3,504)	
Ruby (594)	
Scanner (1,631)	
Security Tool (7,777)	
Shell (3,103)	
Shellcode (1,204)	
Sniffer (886)	

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

- Spoof (2,166)

SQL Injection (16,102)

TCP (2,379)

Trojan (686)

UDP (876)

Virus (662)

Vulnerability (31,136)

Web (9,365)

Whitepaper (3,729)

x86 (946)

XSS (17,494)

Other

SUSE (1,444)

Ubuntu (8,199)

UNIX (9,159)

UnixWare (185)

Windows (6,511)

Other

Site Links

- News by Month

News Tags

Files by Month

File Tags

File Directory

About Us

- History & Purpose

Contact Information

Terms of Service

Privacy Statement

Copyright Information

Hosting By

Rokasec



Follow us on Twitter



Subscribe to an RSS Feed