



CVE-2019-11207

Published on: 08/13/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:35 PM UTC

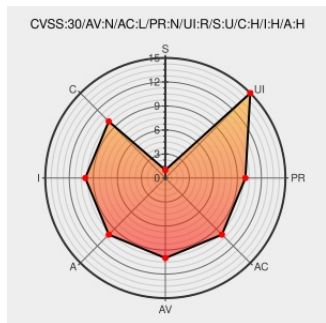
CVE-2019-11207

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Loglogic Enterprise Virtual Appliance](#) from [Tibco](#) contain the following vulnerability:

The web server component of TIBCO Software Inc.'s TIBCO LogLogic Enterprise Virtual Appliance, and TIBCO LogLogic Log Management Intelligence contains multiple vulnerabilities that theoretically allow persistent and reflected cross-site scripting (XSS) attacks, as well as cross-site request forgery (CSRF) attacks. This issue affects: TIBCO

Software Inc. TIBCO LogLogic Enterprise Virtual Appliance version 6.2.1 and prior versions. TIBCO Software Inc. TIBCO LogLogic Log Management Intelligence 6.2.1. TIBCO LogLogic LX825 Appliance 0.0.004, TIBCO LogLogic LX1025 Appliance 0.0.004, TIBCO LogLogic LX4025 Appliance 0.0.004, TIBCO LogLogic MX3025 Appliance 0.0.004, TIBCO LogLogic MX4025 Appliance 0.0.004, TIBCO LogLogic ST1025 Appliance 0.0.004, TIBCO LogLogic ST2025-SAN Appliance 0.0.004, and TIBCO LogLogic ST4025 Appliance 0.0.004 using TIBCO LogLogic Log Management Intelligence versions 6.2.1 and below. TIBCO LogLogic LX1035 Appliance 0.0.005, TIBCO LogLogic LX1025R1 Appliance 0.0.004, TIBCO LogLogic LX1025R2 Appliance 0.0.004, TIBCO LogLogic LX4025R1 Appliance 0.0.004, TIBCO LogLogic LX4025R2 Appliance 0.0.004, TIBCO LogLogic LX4035 Appliance 0.0.005, TIBCO LogLogic ST2025-SANR1 Appliance 0.0.004, TIBCO LogLogic ST2025-SANR2 Appliance 0.0.004, TIBCO LogLogic ST2035-SAN Appliance 0.0.005, TIBCO LogLogic ST4025R1 Appliance 0.0.004, TIBCO LogLogic ST4025R2 Appliance 0.0.004, and TIBCO LogLogic ST4035 Appliance 0.0.005 using TIBCO LogLogic Log Management Intelligence versions 6.2.1 and below.

CVE-2019-11207 has been assigned by security@tibco.com to track the vulnerability - currently rated as **HIGH** severity.

Affected Vendor/Software: **TIBCO Software Inc. - TIBCO LogLogic Enterprise Virtual Appliance** version <= 6.2.1

Affected Vendor/Software: **TIBCO Software Inc. - TIBCO LogLogic Log Management Intelligence** version 6.2.1

CVSS3 Score: **8.8 - HIGH**

Attack
Vector

Attack
Complexity

Privileges
Required

User
Interaction

NETWORK	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH
CVSS2 Score: 6.8 - MEDIUM			
Access Vector	Access Complexity	Authentication	
NETWORK	MEDIUM	NONE	
Confidentiality Impact	Integrity Impact	Availability Impact	
PARTIAL	PARTIAL	PARTIAL	

CVE References		
Description	Tags	Link
TIBCO Security Advisory: August 13, 2019 - TIBCO LogLogic Log Management Intelligence TIBCO Software	Vendor Advisory www.tibco.com text/html	 CONFIRM N/A
Advisory TIBCO Software	Vendor Advisory www.tibco.com text/html	 MISC www.tibco.com/services/support/advisories

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Application	Tibco	Loglogic Enterprise Virtual Appliance	All	All	All	All
Application	Tibco	Loglogic Log Management Intelligence	All	All	All	All
Hardware 	Tibco	Loglogic Lx1025	-	All	All	All
Hardware 	Tibco	Loglogic Lx1025	-	All	All	All
Hardware 	Tibco	Loglogic Lx1025r1	-	All	All	All
Hardware 	Tibco	Loglogic Lx1025r1	-	All	All	All
Operating System	Tibco	Loglogic Lx1025r1 Firmware	0.0.004	All	All	All
Operating System	Tibco	Loglogic Lx1025r1 Firmware	0.0.004	All	All	All
Hardware 	Tibco	Loglogic Lx1025r2	-	All	All	All

Hardware  	Tibco	Loglogic Lx1025r2	-	All	All	All
Operating System	Tibco	Loglogic Lx1025r2 Firmware	0.0.004	All	All	All
Operating System	Tibco	Loglogic Lx1025r2 Firmware	0.0.004	All	All	All
Operating System	Tibco	Loglogic Lx1025 Firmware	0.0.004	All	All	All
Operating System	Tibco	Loglogic Lx1025 Firmware	0.0.004	All	All	All
Hardware  	Tibco	Loglogic Lx1035	-	All	All	All
Hardware  	Tibco	Loglogic Lx1035	-	All	All	All
Operating System	Tibco	Loglogic Lx1035 Firmware	0.0.005	All	All	All
Operating System	Tibco	Loglogic Lx1035 Firmware	0.0.005	All	All	All
Hardware  	Tibco	Loglogic Lx4025	-	All	All	All
Hardware  	Tibco	Loglogic Lx4025	-	All	All	All
Hardware  	Tibco	Loglogic Lx4025r1	-	All	All	All
Hardware  	Tibco	Loglogic Lx4025r1	-	All	All	All
Operating System	Tibco	Loglogic Lx4025r1 Firmware	0.0.004	All	All	All
Operating System	Tibco	Loglogic Lx4025r1 Firmware	0.0.004	All	All	All
Hardware  	Tibco	Loglogic Lx4025r2	-	All	All	All
Hardware  	Tibco	Loglogic Lx4025r2	-	All	All	All
Operating System	Tibco	Loglogic Lx4025r2 Firmware	0.0.004	All	All	All
Operating System	Tibco	Loglogic Lx4025r2 Firmware	0.0.004	All	All	All
Operating System	Tibco	Loglogic Lx4025 Firmware	0.0.004	All	All	All
Operating System	Tibco	Loglogic Lx4025 Firmware	0.0.004	All	All	All
Hardware  	Tibco	Loglogic Lx4035	-	All	All	All
Hardware  	Tibco	Loglogic Lx4035	-	All	All	All
Operating System	Tibco	Loglogic Lx4035 Firmware	0.0.005	All	All	All
Operating System	Tibco	Loglogic Lx4035 Firmware	0.0.005	All	All	All
Hardware  	Tibco	Loglogic Lx825	-	All	All	All

Hardware  	Tibco	Loglogic Lx825	-	All	All	All
Operating System	Tibco	Loglogic Lx825 Firmware	0.0.004	All	All	All
Operating System	Tibco	Loglogic Lx825 Firmware	0.0.004	All	All	All
Hardware  	Tibco	Loglogic Mx3025	-	All	All	All
Hardware  	Tibco	Loglogic Mx3025	-	All	All	All
Operating System	Tibco	Loglogic Mx3025 Firmware	0.0.004	All	All	All
Operating System	Tibco	Loglogic Mx3025 Firmware	0.0.004	All	All	All
Hardware  	Tibco	Loglogic Mx4025	-	All	All	All
Hardware  	Tibco	Loglogic Mx4025	-	All	All	All
Operating System	Tibco	Loglogic Mx4025 Firmware	0.0.004	All	All	All
Operating System	Tibco	Loglogic Mx4025 Firmware	0.0.004	All	All	All
Hardware  	Tibco	Loglogic St1025	-	All	All	All
Hardware  	Tibco	Loglogic St1025	-	All	All	All
Operating System	Tibco	Loglogic St1025 Firmware	0.0.004	All	All	All
Operating System	Tibco	Loglogic St1025 Firmware	0.0.004	All	All	All
Hardware  	Tibco	Loglogic St2025-san	-	All	All	All
Hardware  	Tibco	Loglogic St2025-san	-	All	All	All
Hardware  	Tibco	Loglogic St2025-sanr1	-	All	All	All
Hardware  	Tibco	Loglogic St2025-sanr1	-	All	All	All
Operating System	Tibco	Loglogic St2025-sanr1 Firmware	0.0.004	All	All	All
Operating System	Tibco	Loglogic St2025-sanr1 Firmware	0.0.004	All	All	All
Hardware  	Tibco	Loglogic St2025-sanr2	-	All	All	All
Hardware  	Tibco	Loglogic St2025-sanr2	-	All	All	All
Operating System	Tibco	Loglogic St2025-sanr2 Firmware	0.0.004	All	All	All
Operating System	Tibco	Loglogic St2025-sanr2 Firmware	0.0.004	All	All	All
Operating System	Tibco	Loglogic St2025-san Firmware	0.0.004	All	All	All
Operating	Tibco	Loglogic St2025-san Firmware	0.0.004	All	All	All

cpe:2.3:o:tibco:loglogic_lx1025r1_firmware:0.0.004:*:*:*:*:*:

cpe:2.3:o:tibco:loglogic_lx1025r1_firmware:0.0.004:*:*:*:*:*:

cpe:2.3:h:tibco:loglogic_lx1025r2:-:*:*:*:*:*:

cpe:2.3:h:tibco:loglogic_lx1025r2:-:*:*:*:*:*:*:

```
cpe:2.3:o:tibco:loglogic_lx1025r2_firmware:0.0.004.*:*:*:*:*:
```

cpe:2.3:o:tibco:loglogic_lx1025r2_firmware:0.0.004.*:*:*:*:*:

cpe:2.3:o:tibco:loglogic_lx1025_firmware:0.0.004:*:*:*:*:*:

cpe:2.3:o:tibco:loglogic_lx1025_firmware:0.0.004:*:*:*:*:*:

cpe:2.3:h:tibco:loglogic_lx1035:-:*:*:*:*:*:*:

cpe:2.3:h:tibco:loglogic_lx1035:-:*:*:*:*:*:*:

```
cpe:2.3:o:tibco:loglogic_lx1035_firmware:0.0.005:*:*:*:*:*:
```

```
cpe:2.3:o:tibco:loglogic_lx1035_firmware:0.0.005:*:*:*:*:*:
```

```
cpe:2.3:h:tibco:loglogic_lx4025:-:*:*:*:*:*:*:
```

cpe:2.3:h:tibco:loglogic_lx4025:-:*:*:*:*:*:*:

```
cpe:2.3:h:tibco:loglogic_lx4025r1:-:*:*:*:*:*:
```

```
cpe:2.3:h:tibco:loglogic_lx4025r1:-:*:*:*:*:*:*:
```

cpe:2.3:o:tibco:loglogic_lx4025r1_firmware:0.0.004:*:*:*:*:*:

```
cpe:2.3:o:tibco:loglogic lx4025r1 firmware:0.0.004:*:*:*:*:*:
```

cpe:2.3:h:tibco:loglogic_lx4025r2:-:*:*:*:*:*:*:

```
cpe:2.3:h:tibco:loglogic_lx4025r2:-:*:*:*:*:*:
```

```
cpe:2.3:o:tibco:loglogic_lx4025r2_firmware:0.0.004.*:*:*:*:*:
```

```
cpe:2.3:o:tibco:loglogic lx4025r2 firmware:0.0.004:*:*:*:*:*:
```

cpe:2.3:o:tibco:loglogic_lx4025_firmware:0.0.004.*:*:*:*:*:

```
cpe:2.3:o:tibco:loglogic_lx4025_firmware:0.0.004.*:*:*:*:*:
```

```
cpe:2.3:h:tibco:loglogic_lx4035:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:tibco:loglogic_lx4035:-:*:*:*:*:*:*:
```

cpe:2.3:o:tibco:loglogic_lx4035_firmware:0.0.005:*:*:*:*:*:

```
cpe:2.3:o:tibco:loglogic_lx4035_firmware:0.0.005:*.~*~*~*~*~*~*~*
```

```
cpe:2.3:h:tibco:loglogic_lx825:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:tibco:loglogic_lx825:-:*:*:*:*:*:*:
```

cpe:2.3:o:tibco:loglogic_lx825_firmware:0.0.004:*:*:*:*:*:

cpe:2.3:o:tibco:loglogic_lx825_firmware:0.0.004:*:*:*:*:*:

```
cpe:2.3:h:tibco:loglogic_mx3025:-:*:*:*:*:*:*:
```

cpe:2.3:h:tibco:loglogic_mx3025:-:*:*:*:*:*:*:

cpe:2.3:o:tibco:loglogic_mx3025_firmware:0.0.004:*:*:*:*:*:

cpe:2.3:o:tibco:loglogic_mx3025_firmware:0.0.004:*:*:*:*:*:

cpe:2.3:h:tibco:loglogic_mx4025:-:*:*:*:*:*:*:

```
cpe:2.3:h:tibco:loglogic_mx4025:-:*:*:*:*:*:*:
```

cpe:2.3:o:tibco:loglogic_mx4025_firmware:0.0.004.*:*:*:*:*.*

cpe:2.3:o:tibco:loglogic_mx4025_firmware:0.0.004:*:*:*:*:*:

```
cpe:2.3:h:tibco:loglogic_st1025:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:tibco:loglogic_st1025:-:*:*:*:*:*:
```

```
cpe:2.3:o:tibco:loglogic_st1025_firmware:0.0.004.*:*:*:*:*:
```

```
cpe:2.3:o:tibco:loglogic st1025 firmware:0.0.004:*:*:*:*:*:
```

```
cpe:2.3:h:tibco:loglogic_st2025-san:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:tibco:loglogic_st2025-san:-:*:*:*:*:*:*:
```

```
cpe:2.3:h:tibco:loglogic_st2025-sanr1:-:*:*:*:*:*:
```

```
cpe:2.3:h:tibco:loglogic st2025-sanr1:-:*:*:*:*:*:*:
```

```
cpe:2.3:o:tibco:loglogic_st2025-sanr1_firmware:0.0.004:*:*:*:*.*
```

```
cpe:2.3:o:tibco:loglogic_st2025-sanr1_firmware:0.0.004:*:*:*:*.*
```

```
cpe:2.3:h:tibco:loglogic st2025-sanr2:-:*:*:*:*:*:
```

```
cpe:2.3:h:tibco:loglogic st2025-sanr2:-.*:.*.*.*.*.*.*.*
```

```
cpe:2.3:o:tibco:loglogic st2025-sanr2 firmware:0.0.004:*:*:*:*:*
```

```
cpe:2.3:o:tibco:loglogic st2025-sanr2 firmware:0.0.004:*.~*~*~*~*~*~*
```

```
cpe:2.3:o:tibco:loglogic_st2025-san_firmware:0.0.004:*.***.***.*
```

```
cpe:2.3:o:tibco:loglogic st2025-san firmware:0.0.004:*.***.***.*
```

```
cpe:2.3:h:tibco:loglogic st2035-san:-:*:*:*:*:*:*:
```

cpe:2.3:h:tibco:loglogic_st2035-san:-:*****:
cpe:2.3:o:tibco:loglogic_st2035-san_firmware:0.0.005:*****:
cpe:2.3:o:tibco:loglogic_st2035-san_firmware:0.0.005:*****:
cpe:2.3:h:tibco:loglogic_st4025:-:*****:
cpe:2.3:h:tibco:loglogic_st4025:-:*****:
cpe:2.3:h:tibco:loglogic_st4025r1:-:*****:
cpe:2.3:h:tibco:loglogic_st4025r1:-:*****:
cpe:2.3:o:tibco:loglogic_st4025r1_firmware:0.0.004:*****:
cpe:2.3:o:tibco:loglogic_st4025r1_firmware:0.0.004:*****:
cpe:2.3:h:tibco:loglogic_st4025r2:-:*****:
cpe:2.3:h:tibco:loglogic_st4025r2:-:*****:
cpe:2.3:o:tibco:loglogic_st4025r2_firmware:0.0.004:*****:
cpe:2.3:o:tibco:loglogic_st4025r2_firmware:0.0.004:*****:
cpe:2.3:o:tibco:loglogic_st4025_firmware:0.0.004:*****:
cpe:2.3:o:tibco:loglogic_st4025_firmware:0.0.004:*****:
cpe:2.3:h:tibco:loglogic_st4035:-:*****:
cpe:2.3:h:tibco:loglogic_st4035:-:*****:
cpe:2.3:o:tibco:loglogic_st4035_firmware:0.0.005:*****:
cpe:2.3:o:tibco:loglogic_st4035_firmware:0.0.005:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status status.cve.report