



# CVE-2017-16723

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2017-16723
<b>State</b>	PUBLIC
<b>Assigner</b>	ics-cert@hq.dhs.gov
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-12-11 16:29:00 UTC
<b>Updated</b>	2018-01-02 14:37:00 UTC
<b>Description</b>	A Cross-site Scripting issue was discovered in PHOENIX CONTACT FL COMSERVER BASIC 232/422/485, FL COMSERV

## Risk And Classification

**Problem Types:** CWE-79

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Phoenixcontact	FI Comserver Basic 232	-	All	All	All
Hardware	Phoenixcontact	FI Comserver Basic 232	-	All	All	All
Operating System	Phoenixcontact	FI Comserver Basic 232 Firmware	2.40	All	All	All
Operating System	Phoenixcontact	FI Comserver Basic 232 Firmware	2.40	All	All	All
Hardware	Phoenixcontact	FI Comserver Basic 422	-	All	All	All
Hardware	Phoenixcontact	FI Comserver Basic 422	-	All	All	All
Operating System	Phoenixcontact	FI Comserver Basic 422 Firmware	2.40	All	All	All
Operating System	Phoenixcontact	FI Comserver Basic 422 Firmware	2.40	All	All	All
Hardware	Phoenixcontact	FI Comserver Basic 485	-	All	All	All
Hardware	Phoenixcontact	FI Comserver Basic 485	-	All	All	All
Operating System	Phoenixcontact	FI Comserver Basic 485 Firmware	2.40	All	All	All
Operating System	Phoenixcontact	FI Comserver Basic 485 Firmware	2.40	All	All	All
Hardware	Phoenixcontact	FI Comserver Bas 232	-	All	All	All
Hardware	Phoenixcontact	FI Comserver Bas 232	-	All	All	All
Operating System	Phoenixcontact	FI Comserver Bas 232 Firmware	2.40	All	All	All
Operating System	Phoenixcontact	FI Comserver Bas 232 Firmware	2.40	All	All	All
Hardware	Phoenixcontact	FI Comserver Bas 422	-	All	All	All

Hardware	Phoenixcontact	FI Comserver Bas 422	-	All	All	All
Operating System	Phoenixcontact	FI Comserver Bas 422 Firmware	2.40	All	All	All
Operating System	Phoenixcontact	FI Comserver Bas 422 Firmware	2.40	All	All	All
Hardware	Phoenixcontact	FI Comserver Bas 485-t	-	All	All	All
Hardware	Phoenixcontact	FI Comserver Bas 485-t	-	All	All	All
Operating System	Phoenixcontact	FI Comserver Bas 485-t Firmware	2.40	All	All	All
Operating System	Phoenixcontact	FI Comserver Bas 485-t Firmware	2.40	All	All	All
Hardware	Phoenixcontact	FI Comserver Uni 232	-	All	All	All
Hardware	Phoenixcontact	FI Comserver Uni 232	-	All	All	All
Operating System	Phoenixcontact	FI Comserver Uni 232 Firmware	2.40	All	All	All
Operating System	Phoenixcontact	FI Comserver Uni 232 Firmware	2.40	All	All	All
Hardware	Phoenixcontact	FI Comserver Uni 422	-	All	All	All
Hardware	Phoenixcontact	FI Comserver Uni 422	-	All	All	All
Operating System	Phoenixcontact	FI Comserver Uni 422 Firmware	2.40	All	All	All
Operating System	Phoenixcontact	FI Comserver Uni 422 Firmware	2.40	All	All	All
Hardware	Phoenixcontact	FI Comserver Uni 485	-	All	All	All
Hardware	Phoenixcontact	FI Comserver Uni 485	-	All	All	All
Hardware	Phoenixcontact	FI Comserver Uni 485-t	-	All	All	All
Hardware	Phoenixcontact	FI Comserver Uni 485-t	-	All	All	All
Operating System	Phoenixcontact	FI Comserver Uni 485-t Firmware	2.40	All	All	All
Operating System	Phoenixcontact	FI Comserver Uni 485-t Firmware	2.40	All	All	All
Operating System	Phoenixcontact	FI Comserver Uni 485 Firmware	2.40	All	All	All
Operating System	Phoenixcontact	FI Comserver Uni 485 Firmware	2.40	All	All	All
Hardware	Phoenixcontact	FI Com Server Rs232	-	All	All	All
Hardware	Phoenixcontact	FI Com Server Rs232	-	All	All	All
Operating System	Phoenixcontact	FI Com Server Rs232 Firmware	1.99	All	All	All
Operating System	Phoenixcontact	FI Com Server Rs232 Firmware	1.99	All	All	All
Hardware	Phoenixcontact	FI Com Server Rs485	-	All	All	All
Hardware	Phoenixcontact	FI Com Server Rs485	-	All	All	All
Operating System	Phoenixcontact	FI Com Server Rs485 Firmware	1.99	All	All	All
Operating System	Phoenixcontact	FI Com Server Rs485 Firmware	1.99	All	All	All
Hardware	Phoenixcontact	Psi-modem/eth	-	All	All	All
Operating System	Phoenixcontact	Psi-modem/eth Firmware	2.20	All	All	All
Hardware	Phoenixcontact	Psi-modem/eth	-	All	All	All
Hardware	Phoenixcontact	Psi-modem/eth	-	All	All	All

Operating System	Phoenixcontact	Psi-modem/eth Firmware	2.20	All	All	All
Operating System	Phoenixcontact	Psi-modem/eth Firmware	2.20	All	All	All

## References

Reference	Source	Link
PHOENIX CONTACT FL COMSERVER, FL COM SERVER, and PSI-MODEM/ETH   ICS-CERT	MISC	<a href="https://ics-cert.us-cert.gov">ics-cert.us-cert.gov</a>
Multiple Phoenix Contact Products CVE-2017-16723 Cross Site Scripting Vulnerability	BID	<a href="https://www.securityfocus.com">www.securityfocus.com</a>
PHOENIX CONTACT FL COMSERVER cross-site scripting (XSS) vulnerability — German (Germany)	MISC	<a href="https://cert.vde.com">cert.vde.com</a>
CVE Program record	CVE.ORG	<a href="https://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="https://nvd.nist.gov">nvd.nist.gov</a>

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[590566](#) PHOENIX CONTACT FL COMSERVER, FL COM SERVER, and PSI-MODEM/ETH Cross-Site Scripting (XSS) Vulnerability (ICSA-17-341-03)

© [CVE.report](#) 2026 |

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](https://status.cve.report)