



CVE-2016-5814

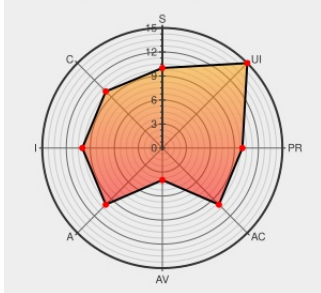
Published on: 09/18/2016 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:27:10 PM UTC

CVE-2016-5814

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H



Certain versions of [Rslogix 500 Professional Edition](#) from [Rockwellautomation](#) contain the following vulnerability:

Buffer overflow in Rockwell Automation RSLogix Micro Starter Lite, RSLogix Micro Developer, RSLogix 500 Starter Edition, RSLogix 500 Standard Edition, and RSLogix 500 Professional Edition allows remote attackers to execute arbitrary code via a crafted RSS project file.

CVE-2016-5814 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.6 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **9.3 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Rockwell Automation RSLogix 500 AND RSLogix Micro File Parser Buffer Overflow Vulnerability ICS-CERT	Mitigation Patch Third Party Advisory US Government Resource ics-cert.us-cert.gov	MISC ics-cert.us-cert.gov/advisories/ICSA-16-224-02

[text/html](#)

No Description Provided

[cve.report \(archive\)](#) [BID 92983](#)[text/html](#)

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	Rockwellautomation	Rslogix 500 Professional Edition	-	All	All	All
Application	Rockwellautomation	Rslogix 500 Professional Edition	-	All	All	All
Application	Rockwellautomation	Rslogix 500 Standard Edition	-	All	All	All
Application	Rockwellautomation	Rslogix 500 Standard Edition	-	All	All	All
Application	Rockwellautomation	Rslogix 500 Starter Edition	-	All	All	All
Application	Rockwellautomation	Rslogix 500 Starter Edition	-	All	All	All
Application	Rockwellautomation	Rslogix Micro Developer	-	All	All	All
Application	Rockwellautomation	Rslogix Micro Developer	-	All	All	All
Application	Rockwellautomation	Rslogix Micro Starter Lite	-	All	All	All
Application	Rockwellautomation	Rslogix Micro Starter Lite	-	All	All	All

cpe:2.3:a:rockwellautomation:rslogix_500_professional_edition:-:*.***.***.*:

cpe:2.3:a:rockwellautomation:rslogix_500_professional_edition:-:*.***.***.*:

cpe:2.3:a:rockwellautomation:rslogix_500_standard_edition:-:*.***.***.*:

cpe:2.3:a:rockwellautomation:rslogix_500_standard_edition:-:*.***.***.*:

cpe:2.3:a:rockwellautomation:rslogix_500_starter_edition:-:*.***.***.*:

cpe:2.3:a:rockwellautomation:rslogix_500_starter_edition:-:*.***.***.*:

cpe:2.3:a:rockwellautomation:rslogix_micro_developer:-:*.***.***.*:

cpe:2.3:a:rockwellautomation:rslogix_micro_developer:-:*.***.***.*:

cpe:2.3:a:rockwellautomation:rslogix_micro_starter_lite:-:*.***.***.*:

cpe:2.3:a:rockwellautomation:rslogix_micro_starter_lite:-:*.***.***.*:

No vendor comments have been submitted for this CVE

© [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](#)