



# Schneider Electric ProClima Command Injection

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2014-9188
<b>State</b>	PUBLISHED
<b>Assigner</b>	icscert
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2014-12-27 15:59:04 UTC
<b>Updated</b>	2026-05-06 22:30:45 UTC
<b>Description</b>	Buffer overflow in an ActiveX control in MDraw30.ocx in Schneider Electric ProClima before 6.1.7 allows remote attackers to

## Risk And Classification

**Primary CVSS:** v2.0 9 from nvd@nist.gov

AV:N/AC:L/Au:N/C:C/I:P/A:P

**Problem Types:** CWE-77 | CWE-119 | CWE-77 CWE-77

Version	Source	Type	Score	Severity	Vector
2.0	nvd@nist.gov	Primary	9		AV:N/AC:L/Au:N/C:C/I:P/A:P
2.0	ics-cert@hq.dhs.gov	Secondary	10		AV:N/AC:L/Au:N/C:C/I:C/A:C
2.0	CNA	CVSS	10		AV:N/AC:L/Au:N/C:C/I:C/A:C

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Complete

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:C/I:P/A:P

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Schneider Electric</a>	<a href="#">Proclima</a>	All	All	All	All

## Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	<a href="#">Schneider Electric</a>	<a href="#">ProClima</a>	affected 6.0.1 custom	Not specified

## References

Reference	Source	Link
<a href="http://download.schneider-electric.com/files">download.schneider-electric.com/files</a>	af854a3a-2127-422b-91ae-364da2661108	<a href="http://download.schneider-electric.com/files">download.schneider-electric.com/files</a>
Schneider Electric ProClima Command Injection Vulnerabilities   ICS-CERT	af854a3a-2127-422b-91ae-364da2661108	<a href="http://ics-cert.us-cert.gov">ics-cert.us-cert.gov</a>
<a href="http://www.cisa.gov/news-events/ics-advisories/icsa-14-350-01">www.cisa.gov/news-events/ics-advisories/icsa-14-350-01</a>	ics-cert@hq.dhs.gov	<a href="http://www.cisa.gov">www.cisa.gov</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>

## Vendor Comments And Credit

### Discovery Credit

**CNA:** This vulnerability was reported to ZDI by security researchers Ariele Caltabiano, Andrea Micalizzi, and Brian Gorenc. (en)

## Additional Advisory Data

### Solutions

**CNA:** Schneider Electric has released an updated version of the ProClima software, Version 6.1.7, which mitigates these vulnerabilities. Customers are encouraged to download the new version and update their installations. It is important that customers first uninstall the current version. The new version can be downloaded from Schneider Electric's web site at the following location: [http://www.schneider-electric.com/ww/en/download/document/ProClima\\_software](http://www.schneider-electric.com/ww/en/download/document/ProClima_software) For further information on these vulnerabilities, please see Schneider Electric's security notification (SEVD 2014-344-01) at Schneider Electric's cybersecurity web page: <http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cyber-security-vulnerabilities-sorted.page> <http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cyber-security-vulnerabilities-sorted.page%20>

There are currently no legacy QID mappings associated with this CVE.

© [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](#).

**Free CVE JSON API** [cve.report/api](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)