


Security Research & Advisories

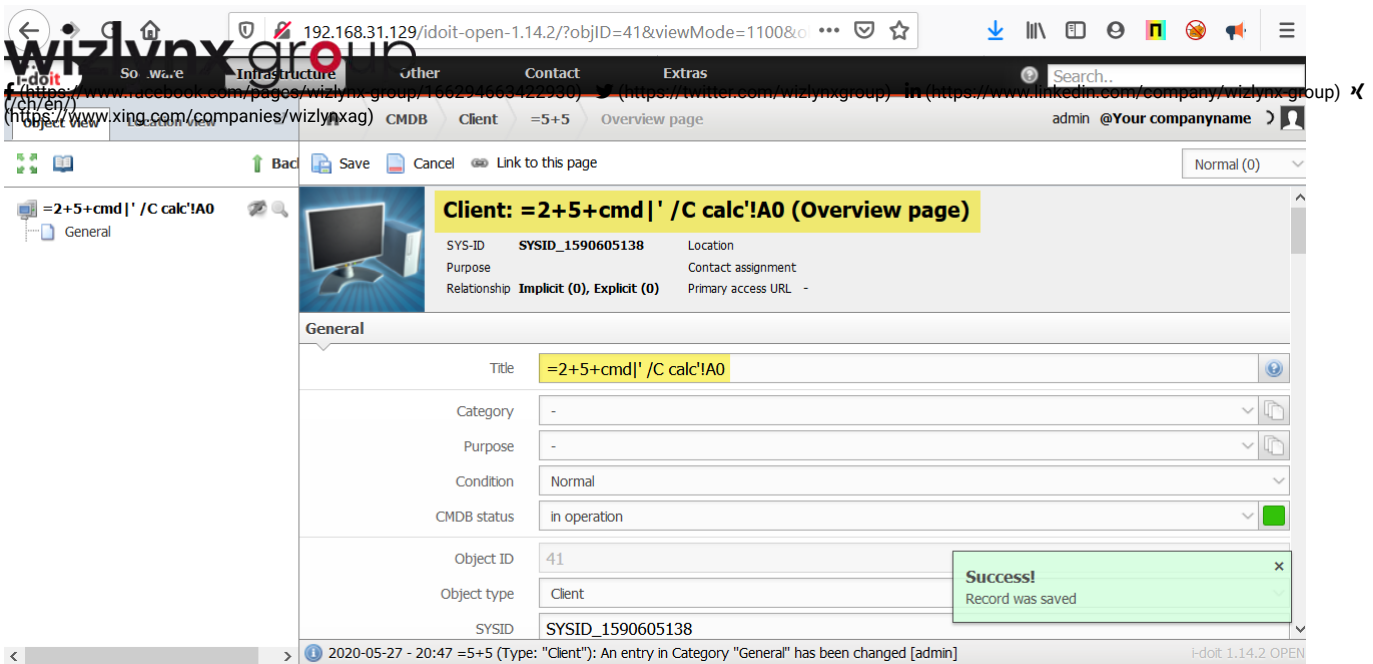
CSV Injection Vulnerability in i-doit 1.14.2

Vendor	 (https://www.i-doit.org/)
Product	phpList
Affected Version(s)	1.14.2 and probably prior
Tested Version(s)	1.14.2
Vendor Notification	May 27, 2020
Advisory Publication	May 27, 2020 [without technical details]
Vendor Fix	Version 1.15
Public Disclosure	August 4, 2020
Latest Modification	August 4, 2020
CVE Identifier(s)	CVE-2020-13826
Product Description	i-doit is a web based IT documentation and CMDB. i-doit documents IT-systems and their changes, defines emergency plans, displays vital information and helps to ensure a stable and efficient IT operation.
Credits	Carlos Ramírez L. Security Researcher & Penetration Tester @wizlynx group

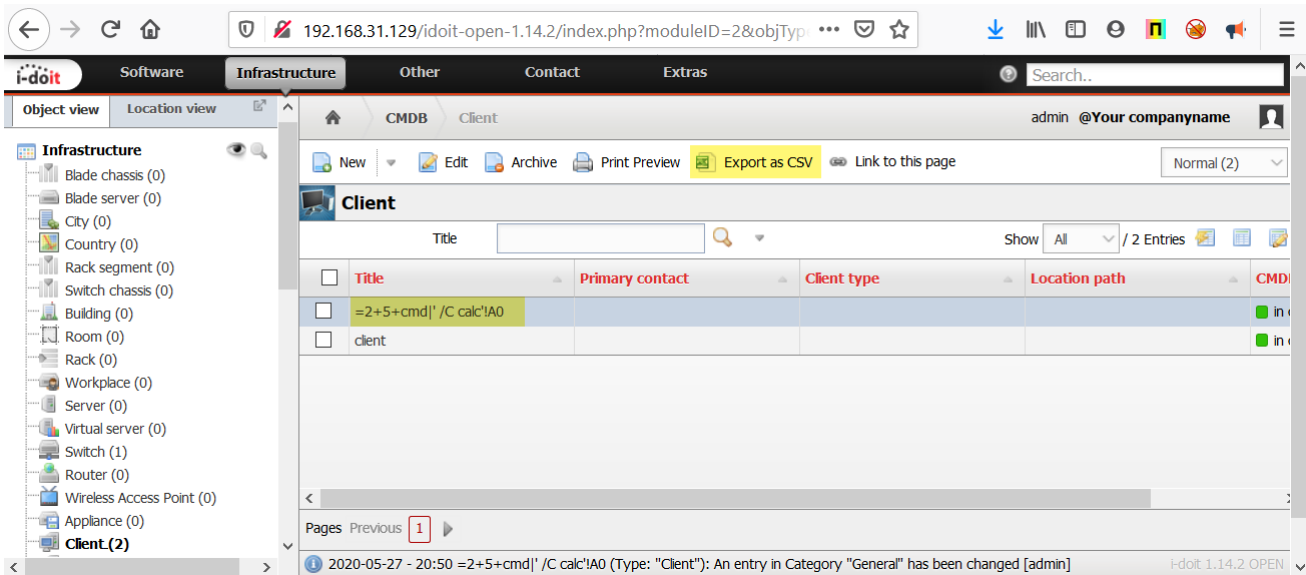
CSV Injection Vulnerability in i-doit 1.14.2			
Severity: Medium ⓘ	CVSS Score: 6.5	CWE-ID: CWE-434 (https://cwe.mitre.org/data/definitions/434)	Status: Not Fixed
Vulnerability Description			
The i-doit web application is affected by CSV Injection vulnerability affecting version 1.14.2 and probably prior versions. An attacker can use the vulnerability to inject malicious code into CSV files in order to gain control over the user's computer, taking advantage of the user's tendency to ignore security warnings in spreadsheets they have downloaded from their own website and exfiltrate the contents of the spreadsheet, or other open spreadsheets.			
CVSS Base Score			
Attack Vector	Network	Scope	Changed
Attack Complexity	Low	Confidentiality Impact	Low
Privileges Required	Low	Integrity Impact	Low
User Interaction	Required	Availability Impact	Low

The application i-doit allows to export the content of the objects created in a CSV file, which allowed an attacker to inject malicious code due to the lack of input validation and output encoding.

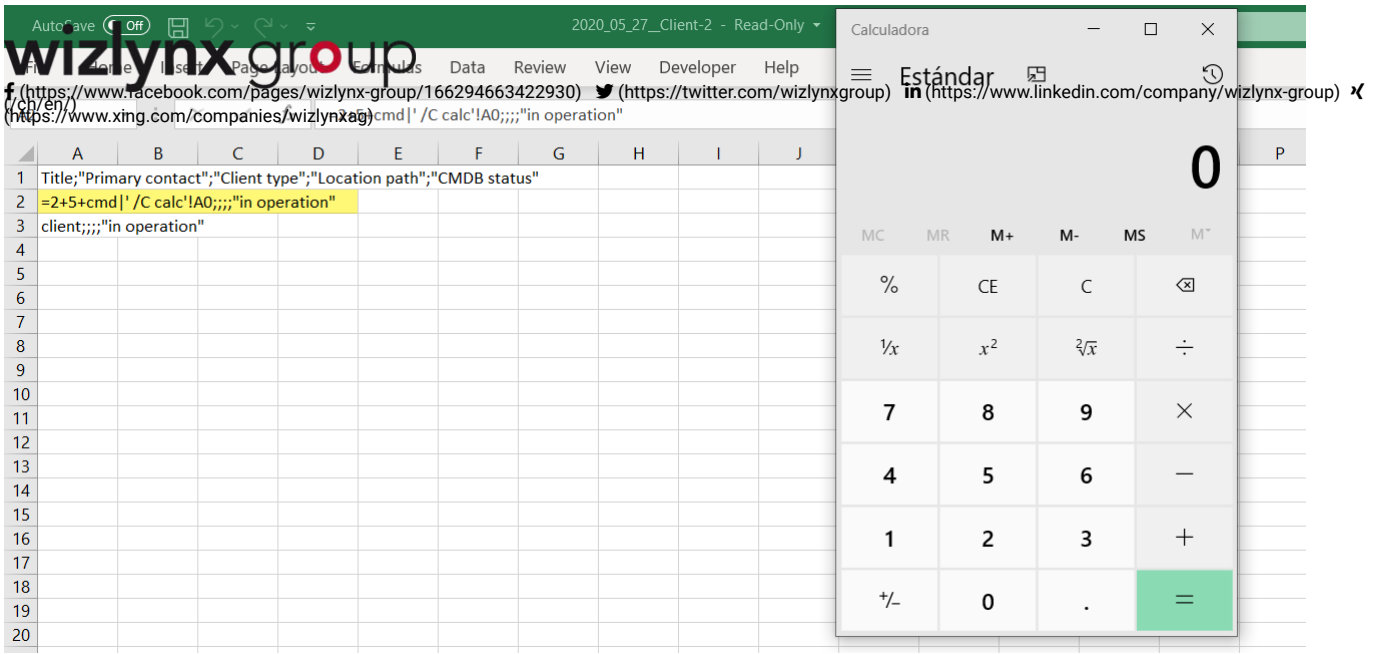
The objects' parameters are copied and exported in CSV files that can be interpreted by the affected user's computer. The payload =cmd|' /C calc 'A0 was submitted as the name of the title object, as shown below:



The code is stored without modifications, and the application allows to download the control and configuration of the objects in CSV format.



As shown in the following screenshot, the malicious payload is executed and in our demonstration Microsoft Calculator is opening on the administrator's machine.



wizlynx group

wizlynx has not only built a solid foundation of information security, quality and project management know-how, but our associates are known for their ability to apply the right soft skills at the right time to best serve our customers. We make it a point to understand the infrastructure, needs and challenges of our customers, which enables us to deliver fast, effective and high quality results. It is our belief that this level of understanding can only be obtained with the most capable and experienced resources. Reach out to our associates at any time through our interactive competence centers to draw upon our knowledge of processes, procedures, guidelines and tools. You'll be able to see, firsthand, the value our team will add to your organization.