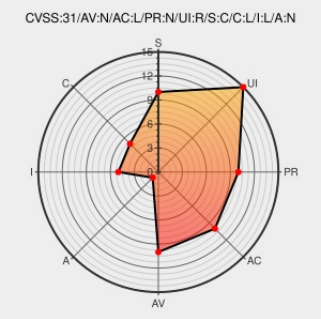
CVE-2022-48325

Published on: Not Yet Published

Last Modified on: 02/27/2023 04:22:00 PM UTC

CVE-2022-48325

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Map-os from Mapos contain the following vulnerability:

Multiple Cross Site Scripting (XSS) vulnerabilities in Mapos 4.39.0 allow attackers to execute arbitrary code. Affects the following parameters: (1) year, (2) oldSenha, (3) novaSenha, (4) termo, (5) nome, (6) cnpj, (7) ie, (8) cep, (9) logradouro, (10) numero, (11) bairro, (12) cidade, (13) uf, (14) telefone, (15) email, (16) id, (17) app_name, (18) per_page, (19) app_theme, (20) os_notification, (21) email_automatico, (22) control_estoque, (23) notifica_whats, (24) control_baixa, (25) control_editos, (26) control_edit_vendas, (27) control_datatable, (28) pix_key, (29) os_status_list, (30) control_2vias, (31) status, (32) start, (33) end in file application/controllers/Mapos.php; (34) token, (35) senha, (36) email, (37) nomeCliente, (38) documento, (39) telefone, (40) celular, (41) rua, (42) numero, (43) complemento, (44) bairro, (45) cidade, (46) estado, (47) cep, (48) idClientes, (49) descricaoProduto, (50) defeito in file application/controllers/Mine.php; (51) pesquisa, (52) status, (53) data, (54) data2, (55) dataInicial, (56) dataFinal, (57) termoGarantia, (58) garantias_id, (59) clientes_id, (60) usuarios_id, (61) idOs, (62) garantia, (63) descricaoProduto, (64) defeito, (65) observacoes, (66) laudoTecnico, (67) id, (68) preco, (69) quantidade, (70) idProduto, (71) idOsProduto, (72) produto, (73) idServico, (74) idOsServico, (75) desconto, (76) tipoDesconto, (77) resultado, (78) vencimento, (79) recebimento, (80) os_id, (81) valor, (82) recebido, (83) formaPgto, (84) tipo, (85) anotacao, (86) idAnotacao in file application/controllers/Os.php.

CVE-2022-48325 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**

CHANGED | LOW | LOW | NONE

CVE References

Description	Tags	Link
Add True for all the post and get inputs by enferas · Pull Request #2015 · RamonSilva20/mapos · GitHub	github.com text/html	MISC github.com/RamonSilva20/mapos/pull/2015#pullrequestreview-1271395780
Multiple possible XSS vulnerabilities · Issue #2010 · RamonSilva20/mapos · GitHub	github.com text/html	MISC github.com/RamonSilva20/mapos/issues/2010
XSS_in_mapos · GitHub	gist.github.com text/html	MISC gist.github.com/enferas/7c7f0a3c6cb30939d9039043c0b86ea8

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	Mapos	Map-os	4.39.0	All	All	All

cpe:2.3:a:mapos:map-os:4.39.0:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-48325 : Multiple Cross Site Scripting #XSS vulnerabilities in Mapos 4.39.0 allow attackers to execute ar… twitter.com/i/web/status/1…	2023-02-16 21:13:05
/r/netcve	CVE-2022-48325	2023-02-16 21:38:58

← Previous ID | Next ID→

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