



CVE-2022-48327

Published on: Not Yet Published

Last Modified on: 02/27/2023 03:28:00 PM UTC

CVE-2022-48327

[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) dataInicial, (2) dataFinal, (3) tipocliente, (4) format, (5) precoInicial, (6) precoFinal, (7) estoqueInicial, (8) estoqueFinal, (9) de_id, (10) ate_id, (11) clientes_id, (12) origem, (13) cliente, (14)

responsavel, (15) status, (16) tipo, (17) situacao in file application/controllers/Relatorios.php; (18) preco, (19) nome, (20) descricao, (21) idServicos, (22) id in file application/controllers/Servicos.php; (23) senha, (24) permissoes_id, (25) idUsuarios, (26) situacao, (27) nome, (28) rg, (29) cpf, (30) cep, (31) rua, (32) numero, (33) bairro, (34) cidade, (35) estado, (36) email, (37) telefone, (38) celular in file application/controllers/Usuarios.php; (39) dataVenda, (40) observacoes, (41) observacoes_cliente, (42) clientes_id, (43) usuarios_id, (44) idVendas, (45) id, (46) idVendasProduto, (47) preco, (48) quantidade, (49) idProduto, (50) produto, (51) desconto, (52) tipoDesconto, (53) resultado, (54) vendas_id, (55) vencimento, (56) recebimento, (57) valor, (58) recebido, (59) formaPgto, (60) tipo in file application/controllers/Vendas.php; (61) situacao, (62) periodo, (63) vencimento_de, (64) vencimento_ate, (65) tipo, (66) status, (67) cliente in file application/views/financeiro/lancamentos.php; (68) year in file application/views/mapos/painel.php; (69) pesquisa in file application/views/os/os.php; (70) etiquetaCode in file application/views/relatorios/imprimir/imprimirEtiquetas.php.

CVE-2022-48327 has been assigned by [M](#) 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-2022-48327 : 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 21:13:37
/r/netcve	CVE-2022-48327	2023-02-16 21:38:59

← Previous ID

Next ID →