# Bugs in OpenSSH

## 1.1 CVE-2016-0777 - Information Leak

OpenSSH client versions between 5.4 and 7.1 are vulnerable to an information leak. The information leak occurs due to an experimental *roaming* feature enabled by default. The *roaming* feature allows a client to buffer input and re-send the buffer to an OpenSSH server on re-connect. This feature, however, uses an unsafe `malloc` call to allocate a buffer on the heap. A potential attacker may be able to read data from a previously de-allocated buffer, including private keys of the client [2].

The immediate remedial action is to update `ssh_config` (global, or all local) and include `UseRoaming no` to disable the roaming feature. Alternatively, all `ssh` sessions can be executed with the `UseRomaing no` flag. The second immediate remedial action is to re-issue all private keys as the attack may have been exploited in the ’wild’ allowing for an attacker to have already stolen the private key.

## 1.2 CVE-2016-0778 - Buffer Overflow

OpenSSH client versions 5.x, 6.x and 7.1.p2 [1] are vulnerable to a file descriptor heap buffer overflow causing a denial of service or arbitrary code execution [3]. In order for this vulnerability to be exploited, two non-default configurations of the OpenSSH client are required - ”ProxyCommand, and either ForwardAgent (-A) or ForwardX11 (-X)” [2].

The immediate remedial action is the same as for *CVE-2016-0777*, `roaming` should be disabled and private keys should be re-issued.

# 2

A CVSS score is an attempt at standardization of the seriousness of a vulnerability given its *exploitability metrics*. The scores range from 0 to 10 with 10 being the most severe. Each metric contributes to the overall seriousness of an exploit, the total being used as the *base score*.

## Exploitability Metrics

1. Attack Vector (AV)
   - (a) Network (AV:N)
   - (b) Adjacent Network (AV:A)
   - (c) Local (AV:L)
   - (d) Physical (AV:P)
2. Access Complexity (AC)
   - (a) Low (AC:L)
   - (b) High (AC:H)
3. Privileges Required (PR)
   - (a) None (PR:N)
   - (b) Low (PR:L)
   - (c) High (PR:H)
4. User Interaction (UI)
   - (a) None (UI:N)
   - (b) Required (UI:R)
5. Scope (S)
   - (a) Unchanged (S:U)
   - (b) Changed (S:C)

6. Confidentiality Impact (C)
   - (a) None (C:N)
   - (b) Low (C:L)
   - (c) High (C:H)
7. Integrity Impact (I)
   - (a) None (I:N)
   - (b) Low (I:L)
   - (c) High (I:H)
8. Availability Impact (A)
   - (a) None (A:N)
   - (b) Low (A:L)
   - (c) High (A:H)

*CVE-2016-0777* can be exploited over the network (AV:N), an attacker can expect repeated success of the attack as the complexity is low (AC:L), the exploit only requires user permissions (PR:L), it does not require any user interaction (UI:N), it comprises high confidentiality impact (C:H), there is no integrity impact (I:N) and it does not affect availability (A:N). The CVE is characterized as having severity of *Medium (4.0-6.9).*

*CVE-2016-0778* can be exploited over the network (AV:N), it is low in exploit complexity (AC:L), does not require any special privilege (PR:N), no user interaction is required (UI:N) and the impact is high for confidentiality (C:H), high for integrity (I:H) and high for availability (A:H). The CVE is characterized with severity *Cricial (9.0 - 10.0).*

CVE-2016-0778 is more severe based on the score.

# 3

# References

[1] National Vulnerability Database. Vulnerability summary for cve-2016-0778. `https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0778`, 2016.

[2] Qualis.com. Roaming through the openssh client: Cve-2016-0777 and cve-2016-0778. `https://www.qualys.com/2016/01/14/cve-2016-0777-cve-2016-0778/openssh-cve-2016-0777-cve-2016-0778.txt`, 2016.

[3] RedHat. Cve-2016-0778. `https://access.redhat.com/security/cve/cve-2016-0778`, 2016.