This communication provides additional information on the Fedora infrastructure intrusion first reported on August 14, 2008. In part this communication reiterates information provided in previous announcements.

On August 12, 2008, a failed cron job on a Fedora host reported an error to the Fedora system administrators. While investigating the source of this error, the sysadmins reviewed the recent logs and discovered that the package complement on the host had changed. Further investigation showed that changes were the result of tampering by an intruder. Once the extent of the problem was discovered, we notified the community:

https://www.redhat.com/archives/fedora-announce-list/2008-August/msg00008.html

The compromise was not the result of a software vulnerability, and as we have previously stated, our investigation has revealed no such vulnerabilities. Instead, the intruder took a copy of a SSH private key which was not secured with a passphrase from a system outside the Fedora infrastructure. The intruder then used that key, which belonged to a Fedora administrator, to access Fedora systems. In addition, based on system log sudo entries, we believe the intruder also compromised that user's password. New security policies for Fedora administrators directly address the further safeguarding of keys, as noted below.

The Fedora package signing key was present on a system to which the intruder had access during the time of the event, but the results of our investigation did not lead us to believe the intruder accessed the key.

The intruder used the account's privileges to build modified versions of openssh and rpm. These packages would have allowed the intruder to capture the passphrases of unwitting users on our build system, or the passphrase used to secure the package signing key. With the signing key's passphrase and access to that key, the intruder would have been able to fraudulently sign packages.

The intruder did deploy the modified packages, and the modified SSH package may have captured passphrases for a short time. However, the investigation supports the conclusion that the modified packages were discovered before anyone accessed the system to sign any packages using the modified RPM package. Therefore, we do not believe the intruder ever had access to the passphrase to the signing key. Nevertheless, previous announcements have explained clearly the precautionary reasons for our earlier decision to deploy a new package signing key. Details on the process and progress of the signing key changes can be found here:

https://fedoraproject.org/wiki/New_signing_key

The modified packages were only installed on a small number of Fedora infrastructure systems, and therefore we do not believe Fedora account holders were at significant risk during the time the intruder had these packages in place. We also required passphrase and SSH key changes from Fedora users, to increase our confidence going forward.

To reiterate, our analysis supports our initial findings that the

Fedora Project infrastructure delivered no software compromised by the intruder to any of its mirrors, or the master repository from which they synchronize content. Our investigation also shows that the intrusion affected only a few internal Fedora infrastructure servers. Most of the mitigation work done by the Fedora Infrastructure team was precautionary, and allows us to have higher confidence in our present and future work.

The Fedora Infrastructure team quickly responded to the threat, isolated the systems in question from the network, made snapshots of affected hosts, assessed the damage, and proceeded to rebuild Fedora's entire infrastructure essentially from scratch. By the end of the first week after the event, most essential systems were functioning nominally again. The remainder of the work took close to three weeks to complete fully, and return all systems to normal status.

To increase our security posture, the Fedora Infrastructure team now requires all members of the Fedora system administrator groups to use passphrases on their private keys. That policy is found, along with other policies of the Infrastructure team, here:

http://infrastructure.fedoraproject.org/csi/security-policy/

The Infrastructure team is also actively developing a Community Services Infrastructure project (http://fedorahosted.org/csi) and supporting documentation to include these lessons in their guidance. Team members have also worked on deploying SELinux throughout our infrastructure as well as an audit and prelude intrusion detection system for added good measure. Furthermore, the Fedora release engineering team is also leading efforts on further improvements and refinements to Fedora's package signing system and procedures. Community members are invited to contact the appropriate Fedora team if they wish to get involved in any of these processes.

The specific facts that emerged during the investigation, which was international in nature, made it necessary to restrict information flowing to the public, to avoid damaging the effectiveness of the investigation. That restriction has been unfortunate, and is not in the ordinary spirit of openness and transparency with which we strive to define the Fedora Project.

We appreciate the patience and support the Fedora community has given us over the past several months. We also wish to express our thanks for the technical assistance of the security response team at Red Hat. This report concludes the matter from the Fedora Project's perspective, and provides a final accounting of the intrusion event and response by the Fedora infrastructure and management teams.

Following is a detailed time line, in UTC, of activities by Fedora contributors.

= = = = =
2008-08-12 01:00:00 - Last packaging signing process from a Fedora admin. Key would have been on host temporarily up until this time.
2008-08-12 07:49:05 - Standard Fedora 'pkgconfig' package installed by the intruder. This package is required to build an 'openssh' package. Intruder proceeds to build a modified 'openssh' package.
2008-08-12 08:10:46 - modified 'openssh' package installed by intruder.

2008-08-12 17:46:50 - Standard Fedora 'gettext' package installed by intruder. This package is required to build an 'rpm' package.
2008-08-12 20:18:36 - Standard Fedora 'mc' package installed by intruder, possibly for convenience of stealth.
2008-08-12 21:33:59 - Bacula backup started (scheduled job)
2008-08-12 22:01:54 - Bacula backup Ended
2008-08-12 22:31:51 - modified 'rpm' package installed (along with standard Fedora package dependencies for 'rpm').
2008-08-12 22:51:00 - Cron job failed, notified admins.
2008-08-12 22:53:00 - Fedora Infrastructure admins first noticed and started poking around at why RPM had changed.
2008-08-12 23:11:00 - Infrastructure team lead is notified and more prodding begins.
2008-08-12 23:38:00 - Infrastructure team members gather for discussions on dedicated, private IRC channel and conference call.
2008-08-13 01:50:00 - It becomes more clear that a script is not at fault. LVM snapshot taken.
2008-08-13 04:00:14 - Bacula backup (during the intrusion) restored to secure location
2008-08-13 04:04:14 - Discovery of an RPM in /root/.ssh/ provides proof of malicious intent.
2008-08-13 04:05:00 - Red Hat security team notified.
2008-08-13 04:46:00 - Compromised host prohibited from routing out or in. All machines on its network are preventing access from it. Outbound connections logged.
2008-08-13 05:16:00 - Fedora Project Leader notified.
2008-08-13 06:13:00 - Host state saved (Xen guest). We have a running copy of the host as it was without a reboot.
2008-08-13 06:14:00 - Users who have accessed the machine during the intrusion advised to change their passwords and SSH keys.
2008-08-13 10:13:00 - Work continues in concert with Red Hat security team members. Preliminary announcement prepared
2008-08-14 17:36:00 - All passwords and SSH keys disabled.
2008-08-14 23:15:13 - Preliminary announcement to fedora-announce-list, 1+19:11 after initial determination of malicious event.
2008-08-15 02:47:00 - All administrator access forced to shell access only for partial re-enabling of account system.
2008-08-15 12:00:00 - (approximate) Fedora's package build system, koji, patched to revoke all access.
2008-08-15 13:11:00 - Last package build routine allowed to complete before shutdown. Comprehensive verification of the build system database contents begins, comparing against known source for malicious content.
2008-08-16 15:30:03 - Update announcement to fedora-announce-list, 3+11:26 after initial determination of malicious event.
2008-08-17 22:34:00 - Members of sysadmin-web group allowed back on app servers.
2008-08-18 04:06:31 - Primary content verification of build system and CVS completed.
2008-08-18 18:06:00 - CVS admins allowed back on servers, and handle additional verification for hosted projects.
2008-08-19 02:07:45 - Update announcement to fedora-announce-list, 5+22:03 after initial determination of malicious event.
2008-08-19 02:37:00 - Hosted project verification completed, and Fedora Hosted back online.
2008-08-19 20:19:00 - Anonymous access via cvspserver allowed.
2008-08-20 02:53:00 - Writable access to cvs1 reactivated.
2008-08-20 18:35:00 - Koji build system officially open and building again.
2008-08-22 12:00:02 - Update announcement to fedora-announce-list, 9+07:56 after initial determination of malicious event.
2008-09-19 02:41:29 - Update announcement to fedora-announce-list, 37+22:37 after initial determination of malicious event. Investigation and issue resolution continues.
2009-03-30 14:00:00 - Final report to fedora-announce-list, 229+9:56 after initial determination of malicious event.

= = = = =