Opensuse Tumbleweed mit Plasma 5.3

Neuinstallationen von Tumbleweed, der Rolling-Release-Variante von Opensuse, verwenden ab sofort Plasma 5.3 als Standard-Desktop. Die Entwickler halten Plasma 5 mit der jüngsten Version für alltagstauglich – und für eine erhebliche Verbesserung gegenüber dem bislang verwendeten KDE-4-Desktop. Einige andere Linux-Distributionen, darunter Kubuntu, haben in den letzten Monaten ebenfalls auf Plasma 5 umgestellt.

Opensuse-Anwender, die auf Tumbleweed umsteigen wollen, finden auf den Opensuse-Seiten Hilfestellung (siehe c't-Link). Tumbleweed stellt deutlich neuere Programmversionen bereit als die aktuelle Opensuse-Version 13.2, die zudem regelmäßig aktualisiert werden. Dank automatisierter Builds und Qualitätskontrollen soll Tumbleweed ähnlich stabil laufen wie die reguläre Distribution. Die Opensuse-Entwickler empfehlen Tumbleweed für Anwender, die schon etwas Erfahrung mit Opensuse haben. (odi@ct.de)

c't Umstieg auf Tumbleweed: ct.de/yzvd

Plasma 5 zieht in Opensuse ein.

Schlankes Cloud-Linux von Intel

Auf dem OpenStack Summit in Vancouver hat Intel sein Clear Linux vorgestellt, eine schlanke Linux-Distribution zum Einsatz in der Cloud ähnlich Canonicals Snappy Ubuntu Core und VMware Photon. Clear Linux soll besonders darauf optimiert sein, die Möglichkeiten aktueller Intel-Hardware auszunutzen.

Clear Linux ist die Grundlage der Clear Container, die die Vorteile leichtgewichtiger Container mit der Sicherheit „echter" virtueller Maschinen verbinden wollen: Der Mini-Hypervisor kvmtool verpackt die Container in virtuelle Maschinen. Er emuliert jedoch weder Hardware noch eine BIOS- oder UEFI-Firmware, sondern startet direkt den Linux-Kernel. Dadurch soll ein solcher Clear Container in weniger als einer Sekunde starten und nur etwa 20 MByte RAM auf dem Host belegen – das liegt eher in der Größenordnung von Containern als „normalen" virtuellen Maschinen. (odi@ct.de)

c't Clear Linux: ct.de/yzvd

Sicherheitslücke in proFTPD

Über eine Lücke in dem Modul mod_copy des populären FTP-Servers ProFTPD können Angreifer beliebigen Code einschleusen und auf Dateien außerhalb der freigegebenen Verzeichnisse zugreifen. Dazu müssen sie sich nicht einmal angemeldet haben. Exploits für die Schwachstelle CVE-2015-3306 kursieren im Netz und werden bereits eingesetzt. So kann ein Angreifer beispielsweise PHP-Code in das Verzeichnis des Webservers schreiben, um ihn anschließend über seine URL auszuführen, oder Systemdateien wie /etc/passwd auslesen.

Die aktuellen ProFTPD-Versionen 1.3.5 und 1.3.4e vom 15. Mai dieses Jahres sind betroffen; bis Redaktionsschluss war auf proftpd.org noch keine korrigierte Version des FTP-Servers verfügbar. Einige Linux-Distributionen, darunter Debian, liefern jedoch schon fehlerkorrigierte ProFTPD-Pakete als Update aus. (odi@ct.de)