Beispiel einer Information zu Schwachstellen

Die vom DFN-CERT verschickten Informationen zu Schwachstellen haben immer den gleichen Grundaufbau. Unterschieden wird lediglich zwischen einem Kurzformat und einem Langformat.

Das Kurzformat kann genutzt werden, um sich einen schnellen Überblick zu verschaffen und um schnell zu prüfen, ob man selber von einer Schwachstelle betroffen ist. Im Gegensatz dazu enthält das Langformat alle vorhandenen Informationen und hilft, das Problem im Detail zu verstehen. Im Archiv der Informationen zu Schwachstellen steht immer das Langformat zur Verfügung.

Beispiel - Textformat

```
Liebe Kolleginnen und Kollegen,

bitte beachten Sie die Informationen zu den verfügbaren Sicherheitsupdates
oder Workarounds in der folgenden Sicherheitsmeldung.

Historie:

Version 1 (21.05.19):
Neues Advisory


Betroffene Software:

Linux-Kernel < 5.0.17


Betroffene Plattformen:

Fedora 30
Fedora 29
Fedora 28



Bewertung:

Gesamtrisiko (DAF): Gering

Bewertung gemäß CVSS v2:
Basisrisiko (CVSS Base Score): 4.3
Aktuelles Schadenspotenzial (Temporal Score): 3.4

Angriffsvektor (AV): Lokal
Angriffskomplexität (AC): Niedrig
Authentifizierung (Au): Einfach

Auswirkung:
Vertraulichkeit (C): Teilweise
Integrität (I): Teilweise
Verfügbarkeit (A): Teilweise

Ausnutzbarkeit (E): Proof-of-Concept existiert
Verfügbare Gegenmaßnahme (RL): Offizieller Fix
Berichtszuverlässigkeit (RC): Bestätigt

Vektor: AV:L/AC:L/Au:S/C:P/I:P/A:P/E:POC/RL:OF/RC:C
```

Ein lokaler, einfach authentisierter Angreifer kann eine Schwachstelle im Linux-Kernel vermutlich ausnutzen, um einen Denial-of-Service (DoS)-Zustand herbeizuführen.

Für Fedora 28, 29 und 30 stehen Sicherheitsupdates für den Linux-Kernel auf Version 5.0.17 im Status 'testing' bereit, welche die Schwachstelle und eine
Anzahl weiterer Fehler beheben. Nach Installation des Updates ist ein Neustart des Systems erforderlich, damit die durch dieses Update eingebrachten Änderungen wirksam werden.

RED-HAT-BUG-ID-1711194 Schwachstelle in Linux-Kernel ermöglicht nicht spezifizierte Angriffe

In 'drivers/virt/fsl_hypervisor.c' im Linux-Kernel existiert eine Schwachstelle. Der Wert für 'param.count' ist eine Benutzereingabe vom Typ u64. Später wird davon ausgegangen, dass 'param.count' mindestens eins ist, welches zu einer Dereferenzierung von ZERO_SIZE_PTR führt, falls dies nicht der Fall ist. Außerdem kann es zu einem Ganzzahlüberlauf (Integer Overflow) kommen, welcher dazu führt, dass ein kleineres 'pages'-Array definiert wird,
als benötigt.

Liste der Schwachstellen:
RED-HAT-BUG-ID-1711194

Referenzen:

Dieses Advisory finden Sie auch im DFN-CERT Portal unter:
[https://portal.cert.dfn.de/advisories/details/2019-1035]

Zusätzliche Informationen:

Red Hat Bug #1711194 - kernel: assumption of correct user input in drivers/virt/fsl_hypervisor.c leads to integer overflow
bugzilla.redhat.com/show_bug.cgi

Patches:

Fedora Security Update FEDORA-2019-41de525c08 (Fedora 28, kernel-5.0.17-100.fc28)
bodhi.fedoraproject.org/updates/FEDORA-2019-41de525c08

Fedora Security Update FEDORA-2019-8169b57f28 (Fedora 29, kernel-5.0.17-200.fc29)
bodhi.fedoraproject.org/updates/FEDORA-2019-8169b57f28

Fedora Security Update FEDORA-2019-b318b2c6f3 (Fedora 30, kernel-5.0.17-300.fc30)
bodhi.fedoraproject.org/updates/FEDORA-2019-b318b2c6f3

Mit freundlichen Grüßen,
Ihr DFN-CERT Incident Response Team

Beispiel - JSON-Format


```
{
  "version": "1",
  "ref_num": "2019-1035",
  "fieldsets": {
    "scoring": {
      "daf": {
        "risk": "low"
      },
      "cpes": [
        {
          "displayname": "Fedora 30\n",
          "relation": "=",
          "cpe": "cpe:/o:redhat:fedora:30",
          "type": "platform"
        },
        {
          "displayname": "Fedora 29\n",
          "relation": "=",
          "cpe": "cpe:/o:redhat:fedora:29",
          "type": "platform"
        },
        {
          "displayname": "Fedora 28\n",
          "relation": "=",
          "cpe": "cpe:/o:redhat:fedora:28",
          "type": "platform"
        },
        {
          "displayname": "Linux-Kernel < 5.0.17\n",
          "relation": "<",
          "cpe": "cpe:/o:linux:linux_kernel:5.0.17",
          "type": "software"
        }
      ],
      "cvss": {
        "temporal_score": "3.4",
        "vector": "AV:L/AC:L/Au:S/C:P/I:P/A:P/E:POC/RL:OF/RC:C",
        "exploitability_score": "3.1",
        "impact_score": "6.4",
        "base_score": "4.3"
      }
    },
    "basic": {
      "description": "Ein lokaler, einfach authentisierter Angreifer kann
eine Schwachstelle im Linux-Kernel vermutlich ausnutzen, um einen Denial-
of-Service (DoS)-Zustand herbeizuf\u00fchren.\n\nF\u00fcr Fedora 28, 29 und
30 stehen Sicherheitsupdates f\u00fcr den Linux-Kernel auf Version 5.0.17
im Status 'testing' bereit, welche die Schwachstelle und eine Anzahl
weiterer Fehler beheben. Nach Installation des Updates ist ein Neustart des
Systems erforderlich, damit die durch dieses Update eingebrachten
\u00c4nderungen wirksam werden.",
      "workaround": null,
      "created": "20190521T08:08:19",
      "vulnerabilities": [
        {
          "title": "Schwachstelle in Linux-Kernel erm\u00f6glicht nicht
spezifizierte Angriffe",
          "description": "In 'drivers/virt/fsl_hypervisor.c' im Linux-
Kernel existiert eine Schwachstelle. Der Wert f\u00fcr 'param.count' ist
eine Benutzereingabe vom Typ u64. Sp\u00e4ter wird davon ausgegangen, dass
'param.count' mindestens eins ist, welches zu einer Dereferenzierung von
```

```
ZERO_SIZE_PTR f\u00fchrt, falls dies nicht der Fall ist. Au\u00dferdem kann
es zu einem Ganzzahl\u00fcberlauf (Integer Overflow) kommen, welcher dazu
f\u00fchrt, dass ein kleineres 'pages'-Array definiert wird, als
ben\u00f6tigt.",
          "name": "RED-HAT-BUG-ID-1711194"
        }
      ],
      "title": "Linux-Kernel: Eine Schwachstelle erm\u00f6glicht u. a.
einen Denial-of-Service-Angriff",
      "references": [
        {
          "url": "https://bodhi.fedoraproject.org/updates/FEDORA-2019-
41de525c08",
          "type": "patch",
          "description": "Fedora Security Update FEDORA-2019-41de525c08
(Fedora 28, kernel-5.0.17-100.fc28)"
        },
        {
          "url": "https://bodhi.fedoraproject.org/updates/FEDORA-2019-
8169b57f28",
          "type": "patch",
          "description": "Fedora Security Update FEDORA-2019-8169b57f28
(Fedora 29, kernel-5.0.17-200.fc29)"
        },
        {
          "url": "https://bodhi.fedoraproject.org/updates/FEDORA-2019-
b318b2c6f3",
          "type": "patch",
          "description": "Fedora Security Update FEDORA-2019-b318b2c6f3
(Fedora 30, kernel-5.0.17-300.fc30)"
        },
        {
          "url": "https://bugzilla.redhat.com/show_bug.cgi?id=1711194", a
          "type": "info",
          "description": "Red Hat Bug #1711194 - kernel: assumption of
correct user input in drivers/virt/fsl_hypervisor.c leads to integer
overflow"
        }
      ],
      "history": [
        {
          "timestamp": "20190521T14:22:13",
          "version": "1",
          "description": "Neues Advisory"
        }
      ]
    }
  }
}
```