

```

{
  "$schema": "https://schemastore.azurewebsites.net/schemas/json/sarif-2.1.0-rtm.4.json",
  "version": "2.1.0",
  "runs": [
    {
      "tool": {
        "driver": {
          "name": "Anchore Container Vulnerability Report (T0)",
          "fullName": "Anchore Container Vulnerability Report (T0)",
          "version": "0.17.0",
          "semanticVersion": "0.17.0",
          "dottedQuadFileVersion": "0.17.0.0",
          "rules": [
            {
              "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2004-0971_deb_libgssapi-krb5-2_1.18.3-6",
              "shortDescription": {
                "text": "CVE-2004-0971 Negligible vulnerability for libgssapi-krb5-2 package"
              },
              "fullDescription": {
                "text": "Version 1.18.3-6 is affected with no fixes reported yet."
              },
              "help": {
                "text": "Vulnerability CVE-2004-0971\nSeverity: Negligible\nPackage: libgssapi-krb5-2\nVersion: 1.18.3-6\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2004-0971](https://security-tracker.debian.org/tracker/CVE-2004-0971)",
                "markdown": "***Vulnerability CVE-2004-0971**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libgssapi-krb5-2 | 1.18.3-6 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2004-0971](https://security-tracker.debian.org/tracker/CVE-2004-0971) |\n"
              }
            }
          ]
        }
      }
    }
  ]
}

```

```

},
{
  "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2004-0971_deb_libk5crypto3_1.18.3-6",
  "shortDescription": {
    "text": "CVE-2004-0971 Negligible vulnerability for libk5crypto3 package"
  },
  "fullDescription": {
    "text": "Version 1.18.3-6 is affected with no fixes reported yet."
  },
  "help": {
    "text": "Vulnerability CVE-2004-0971\nSeverity: Negligible\nPackage: libk5crypto3\nVersion: 1.18.3-6\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2004-0971](https://security-tracker.debian.org/tracker/CVE-2004-0971)",
    "markdown": "***Vulnerability CVE-2004-0971**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libk5crypto3 | 1.18.3-6 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2004-0971](https://security-tracker.debian.org/tracker/CVE-2004-0971)|\n"
  }
},
{
  "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2004-0971_deb_libkrb5-3_1.18.3-6",
  "shortDescription": {
    "text": "CVE-2004-0971 Negligible vulnerability for libkrb5-3 package"
  },
  "fullDescription": {
    "text": "Version 1.18.3-6 is affected with no fixes reported yet."
  },
  "help": {
    "text": "Vulnerability CVE-2004-0971\nSeverity: Negligible\nPackage: libkrb5-3\nVersion: 1.18.3-6\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2004-0971](https://security-tracker.debian.org/tracker/CVE-2004-0971)",

```

```
"markdown": "***Vulnerability CVE-2004-0971**\n| Severity | Package | Version | Fix Version |  
Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libkrb5-  
3 | 1.18.3-6 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2004-0971](https://security-  
tracker.debian.org/tracker/CVE-2004-0971)|\n"
```

```
}
```

```
},
```

```
{
```

```
"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2004-0971_deb_libkrb5support0_1.18.3-  
6",
```

```
"shortDescription": {
```

```
"text": "CVE-2004-0971 Negligible vulnerability for libkrb5support0 package"
```

```
},
```

```
"fullDescription": {
```

```
"text": "Version 1.18.3-6 is affected with no fixes reported yet."
```

```
},
```

```
"help": {
```

```
"text": "Vulnerability CVE-2004-0971\nSeverity: Negligible\nPackage:  
libkrb5support0\nVersion: 1.18.3-6\nFix Version: none\nType: deb\nLocation:  
/var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2004-0971](https://security-  
tracker.debian.org/tracker/CVE-2004-0971)",
```

```
"markdown": "***Vulnerability CVE-2004-0971**\n| Severity | Package | Version | Fix Version |  
Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libkrb5support0 | 1.18.3-6 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2004-  
0971](https://security-tracker.debian.org/tracker/CVE-2004-0971)|\n"
```

```
}
```

```
},
```

```
{
```

```
"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2005-2541_deb_tar_1.34+dfsg-1",
```

```
"shortDescription": {
```

```
"text": "CVE-2005-2541 Negligible vulnerability for tar package"
```

```
},
```

```
"fullDescription": {
```

```

    "text": "Version 1.34+dfsg-1 is affected with no fixes reported yet."
  },
  "help": {
    "text": "Vulnerability CVE-2005-2541\nSeverity: Negligible\nPackage: tar\nVersion: 1.34+dfsg-1\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2005-2541](https://security-tracker.debian.org/tracker/CVE-2005-2541)",
    "markdown": "***Vulnerability CVE-2005-2541**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | tar | 1.34+dfsg-1 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2005-2541](https://security-tracker.debian.org/tracker/CVE-2005-2541)|\n"
  }
},
{
  "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2007-5686_deb_login_1:4.8.1-1",
  "shortDescription": {
    "text": "CVE-2007-5686 Negligible vulnerability for login package"
  },
  "fullDescription": {
    "text": "Version 1:4.8.1-1 is affected with no fixes reported yet."
  },
  "help": {
    "text": "Vulnerability CVE-2007-5686\nSeverity: Negligible\nPackage: login\nVersion: 1:4.8.1-1\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2007-5686](https://security-tracker.debian.org/tracker/CVE-2007-5686)",
    "markdown": "***Vulnerability CVE-2007-5686**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | login | 1:4.8.1-1 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2007-5686](https://security-tracker.debian.org/tracker/CVE-2007-5686)|\n"
  }
}
{
  "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2007-5686_deb_passwd_1:4.8.1-1",

```

```

"shortDescription": {
  "text": "CVE-2007-5686 Negligible vulnerability for passwd package"
},
"fullDescription": {
  "text": "Version 1:4.8.1-1 is affected with no fixes reported yet."
},
"help": {
  "text": "Vulnerability CVE-2007-5686\nSeverity: Negligible\nPackage: passwd\nVersion: 1:4.8.1-1\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2007-5686](https://security-tracker.debian.org/tracker/CVE-2007-5686)",
  "markdown": "***Vulnerability CVE-2007-5686**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | passwd | 1:4.8.1-1 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2007-5686](https://security-tracker.debian.org/tracker/CVE-2007-5686) |\n"
}
},
{
  "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2007-6755_deb_libssl1.1_1.1.1k-1+deb11u1",
  "shortDescription": {
    "text": "CVE-2007-6755 Negligible vulnerability for libssl1.1 package"
  },
  "fullDescription": {
    "text": "Version 1.1.1k-1+deb11u1 is affected with no fixes reported yet."
  },
  "help": {
    "text": "Vulnerability CVE-2007-6755\nSeverity: Negligible\nPackage: libssl1.1\nVersion: 1.1.1k-1+deb11u1\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2007-6755](https://security-tracker.debian.org/tracker/CVE-2007-6755)",
    "markdown": "***Vulnerability CVE-2007-6755**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libssl1.1 | 1.1.1k-1+deb11u1 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2007-6755](https://security-tracker.debian.org/tracker/CVE-2007-6755) |\n"
  }
}

```

```

    }
  },
  {
    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2007-6755_deb_openssl_1.1.1k-1+deb11u1",
    "shortDescription": {
      "text": "CVE-2007-6755 Negligible vulnerability for openssl package"
    },
    "fullDescription": {
      "text": "Version 1.1.1k-1+deb11u1 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2007-6755\nSeverity: Negligible\nPackage: openssl\nVersion: 1.1.1k-1+deb11u1\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2007-6755](https://security-tracker.debian.org/tracker/CVE-2007-6755)",
      "markdown": "***Vulnerability CVE-2007-6755**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | openssl | 1.1.1k-1+deb11u1 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2007-6755](https://security-tracker.debian.org/tracker/CVE-2007-6755) |\n"
    }
  },
  {
    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2010-0928_deb_libssl1.1_1.1.1k-1+deb11u1",
    "shortDescription": {
      "text": "CVE-2010-0928 Negligible vulnerability for libssl1.1 package"
    },
    "fullDescription": {
      "text": "Version 1.1.1k-1+deb11u1 is affected with no fixes reported yet."
    },
    "help": {

```

```
"text": "Vulnerability CVE-2010-0928\nSeverity: Negligible\nPackage: libssl1.1\nVersion: 1.1.1k-1+deb11u1\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2010-0928](https://security-tracker.debian.org/tracker/CVE-2010-0928)",
```

```
"markdown": "***Vulnerability CVE-2010-0928**\n| Severity | Package | Version | Fix Version |  
Type | Location | Data Namespace | Link |\n| Negligible | libssl1.1 | 1.1.1k-1+deb11u1 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2010-0928](https://security-tracker.debian.org/tracker/CVE-2010-0928) |\n"
```

```
}
```

```
},
```

```
{
```

```
"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2010-0928_deb_openssl_1.1.1k-1+deb11u1",
```

```
"shortDescription": {
```

```
"text": "CVE-2010-0928 Negligible vulnerability for openssl package"
```

```
},
```

```
"fullDescription": {
```

```
"text": "Version 1.1.1k-1+deb11u1 is affected with no fixes reported yet."
```

```
},
```

```
"help": {
```

```
"text": "Vulnerability CVE-2010-0928\nSeverity: Negligible\nPackage: openssl\nVersion: 1.1.1k-1+deb11u1\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2010-0928](https://security-tracker.debian.org/tracker/CVE-2010-0928)",
```

```
"markdown": "***Vulnerability CVE-2010-0928**\n| Severity | Package | Version | Fix Version |  
Type | Location | Data Namespace | Link |\n| Negligible | openssl | 1.1.1k-1+deb11u1 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2010-0928](https://security-tracker.debian.org/tracker/CVE-2010-0928) |\n"
```

```
}
```

```
},
```

```
{
```

```
"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2010-4051_deb_libc-bin_2.31-13",
```

```
"shortDescription": {
```

```
"text": "CVE-2010-4051 Negligible vulnerability for libc-bin package"
```

```
},
```

```

    "fullDescription": {
      "text": "Version 2.31-13 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2010-4051\nSeverity: Negligible\nPackage: libc-bin\nVersion: 2.31-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2010-4051](https://security-tracker.debian.org/tracker/CVE-2010-4051)",
      "markdown": "***Vulnerability CVE-2010-4051**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libc-bin | 2.31-13 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2010-4051](https://security-tracker.debian.org/tracker/CVE-2010-4051)|\n"
    }
  },
  {
    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2010-4051_deb_libc6_2.31-13",
    "shortDescription": {
      "text": "CVE-2010-4051 Negligible vulnerability for libc6 package"
    },
    "fullDescription": {
      "text": "Version 2.31-13 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2010-4051\nSeverity: Negligible\nPackage: libc6\nVersion: 2.31-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2010-4051](https://security-tracker.debian.org/tracker/CVE-2010-4051)",
      "markdown": "***Vulnerability CVE-2010-4051**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libc6 | 2.31-13 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2010-4051](https://security-tracker.debian.org/tracker/CVE-2010-4051)|\n"
    }
  }
}

```



```

    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2010-4052_deb_libc-bin_2.31-13",
    "shortDescription": {
      "text": "CVE-2010-4052 Negligible vulnerability for libc-bin package"
    },
    "fullDescription": {
      "text": "Version 2.31-13 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2010-4052\nSeverity: Negligible\nPackage: libc-bin\nVersion: 2.31-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2010-4052](https://security-tracker.debian.org/tracker/CVE-2010-4052)",
      "markdown": "***Vulnerability CVE-2010-4052**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libc-bin | 2.31-13 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2010-4052](https://security-tracker.debian.org/tracker/CVE-2010-4052) |\n"
    }
  },
  {
    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2010-4052_deb_libc6_2.31-13",
    "shortDescription": {
      "text": "CVE-2010-4052 Negligible vulnerability for libc6 package"
    },
    "fullDescription": {
      "text": "Version 2.31-13 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2010-4052\nSeverity: Negligible\nPackage: libc6\nVersion: 2.31-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2010-4052](https://security-tracker.debian.org/tracker/CVE-2010-4052)",
      "markdown": "***Vulnerability CVE-2010-4052**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |"
    }
  }
}

```

|\n|Negligible|libc6|2.31-13|none|deb|/var/lib/dpkg/status|unknown|[CVE-2010-4052](https://security-tracker.debian.org/tracker/CVE-2010-4052)|\n"

}

},

{

"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2010-4756_deb_libc-bin_2.31-13",

"shortDescription": {

"text": "CVE-2010-4756 Negligible vulnerability for libc-bin package"

},

"fullDescription": {

"text": "Version 2.31-13 is affected with no fixes reported yet."

},

"help": {

"text": "Vulnerability CVE-2010-4756\nSeverity: Negligible\nPackage: libc-bin\nVersion: 2.31-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2010-4756](https://security-tracker.debian.org/tracker/CVE-2010-4756)",

"markdown": "***Vulnerability CVE-2010-4756**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libc-bin | 2.31-13 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2010-4756](https://security-tracker.debian.org/tracker/CVE-2010-4756) |\n"

}

},

{

"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2010-4756_deb_libc6_2.31-13",

"shortDescription": {

"text": "CVE-2010-4756 Negligible vulnerability for libc6 package"

},

"fullDescription": {

"text": "Version 2.31-13 is affected with no fixes reported yet."

},

"help": {

```
    "text": "Vulnerability CVE-2010-4756\nSeverity: Negligible\nPackage: libc6\nVersion: 2.31-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2010-4756](https://security-tracker.debian.org/tracker/CVE-2010-4756)",
```

```
    "markdown": "***Vulnerability CVE-2010-4756**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libc6 | 2.31-13 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2010-4756](https://security-tracker.debian.org/tracker/CVE-2010-4756) |\n"
```

```
  }
```

```
},
```

```
{
```

```
  "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2011-3374_deb_appt_2.2.4",
```

```
  "shortDescription": {
```

```
    "text": "CVE-2011-3374 Negligible vulnerability for apt package"
```

```
  },
```

```
  "fullDescription": {
```

```
    "text": "Version 2.2.4 is affected with no fixes reported yet."
```

```
  },
```

```
  "help": {
```

```
    "text": "Vulnerability CVE-2011-3374\nSeverity: Negligible\nPackage: apt\nVersion: 2.2.4\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2011-3374](https://security-tracker.debian.org/tracker/CVE-2011-3374)",
```

```
    "markdown": "***Vulnerability CVE-2011-3374**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | apt | 2.2.4 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2011-3374](https://security-tracker.debian.org/tracker/CVE-2011-3374) |\n"
```

```
  }
```

```
},
```

```
{
```

```
  "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2011-3374_deb_libapt-pkg6.0_2.2.4",
```

```
  "shortDescription": {
```

```
    "text": "CVE-2011-3374 Negligible vulnerability for libapt-pkg6.0 package"
```

```
  },
```

```

    "fullDescription": {
      "text": "Version 2.2.4 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2011-3374\nSeverity: Negligible\nPackage: libapt-pkg6.0\nVersion: 2.2.4\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2011-3374](https://security-tracker.debian.org/tracker/CVE-2011-3374)",
      "markdown": "***Vulnerability CVE-2011-3374**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libapt-pkg6.0 | 2.2.4 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2011-3374](https://security-tracker.debian.org/tracker/CVE-2011-3374)|\n"
    }
  },
  {
    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2011-3389_deb_libgnutls30_3.7.1-5",
    "shortDescription": {
      "text": "CVE-2011-3389 Medium vulnerability for libgnutls30 package"
    },
    "fullDescription": {
      "text": "Version 3.7.1-5 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2011-3389\nSeverity: Medium\nPackage: libgnutls30\nVersion: 3.7.1-5\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2011-3389](https://security-tracker.debian.org/tracker/CVE-2011-3389)",
      "markdown": "***Vulnerability CVE-2011-3389**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Medium | libgnutls30 | 3.7.1-5 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2011-3389](https://security-tracker.debian.org/tracker/CVE-2011-3389)|\n"
    }
  }
}

```

```

    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2011-4116_deb_perl-base_5.32.1-4+deb11u1",
    "shortDescription": {
        "text": "CVE-2011-4116 Negligible vulnerability for perl-base package"
    },
    "fullDescription": {
        "text": "Version 5.32.1-4+deb11u1 is affected with no fixes reported yet."
    },
    "help": {
        "text": "Vulnerability CVE-2011-4116\nSeverity: Negligible\nPackage: perl-base\nVersion: 5.32.1-4+deb11u1\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2011-4116](https://security-tracker.debian.org/tracker/CVE-2011-4116)",
        "markdown": "***Vulnerability CVE-2011-4116**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | perl-base | 5.32.1-4+deb11u1 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2011-4116](https://security-tracker.debian.org/tracker/CVE-2011-4116)|\n"
    }
},
{
    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2013-0340_deb_libexpat1_2.2.10-2",
    "shortDescription": {
        "text": "CVE-2013-0340 Negligible vulnerability for libexpat1 package"
    },
    "fullDescription": {
        "text": "Version 2.2.10-2 is affected with no fixes reported yet."
    },
    "help": {
        "text": "Vulnerability CVE-2013-0340\nSeverity: Negligible\nPackage: libexpat1\nVersion: 2.2.10-2\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2013-0340](https://security-tracker.debian.org/tracker/CVE-2013-0340)",
        "markdown": "***Vulnerability CVE-2013-0340**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |

```

|\n|Negligible|libexpat1|2.2.10-2|none|deb|/var/lib/dpkg/status|unknown|[CVE-2013-0340](https://security-tracker.debian.org/tracker/CVE-2013-0340)|\n"

}

},

{

"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2013-4235_deb_login_1:4.8.1-1",

"shortDescription": {

"text": "CVE-2013-4235 Negligible vulnerability for login package"

},

"fullDescription": {

"text": "Version 1:4.8.1-1 is affected with no fixes reported yet."

},

"help": {

"text": "Vulnerability CVE-2013-4235\nSeverity: Negligible\nPackage: login\nVersion: 1:4.8.1-1\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2013-4235](https://security-tracker.debian.org/tracker/CVE-2013-4235)",

"markdown": "***Vulnerability CVE-2013-4235**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n|\n|Negligible|login|1:4.8.1-1|none|deb|/var/lib/dpkg/status|unknown|[CVE-2013-4235](https://security-tracker.debian.org/tracker/CVE-2013-4235)|\n"

}

},

{

"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2013-4235_deb_passwd_1:4.8.1-1",

"shortDescription": {

"text": "CVE-2013-4235 Negligible vulnerability for passwd package"

},

"fullDescription": {

"text": "Version 1:4.8.1-1 is affected with no fixes reported yet."

},

"help": {

```
"text": "Vulnerability CVE-2013-4235\nSeverity: Negligible\nPackage: passwd\nVersion: 1:4.8.1-1\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2013-4235](https://security-tracker.debian.org/tracker/CVE-2013-4235)",
```

```
"markdown": "***Vulnerability CVE-2013-4235**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | passwd | 1:4.8.1-1 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2013-4235](https://security-tracker.debian.org/tracker/CVE-2013-4235) |\n"
```

```
}
```

```
},
```

```
{
```

```
"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2013-4392_deb_libsystemd0_247.3-6",
```

```
"shortDescription": {
```

```
"text": "CVE-2013-4392 Negligible vulnerability for libsystemd0 package"
```

```
},
```

```
"fullDescription": {
```

```
"text": "Version 247.3-6 is affected with no fixes reported yet."
```

```
},
```

```
"help": {
```

```
"text": "Vulnerability CVE-2013-4392\nSeverity: Negligible\nPackage: libsystemd0\nVersion: 247.3-6\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2013-4392](https://security-tracker.debian.org/tracker/CVE-2013-4392)",
```

```
"markdown": "***Vulnerability CVE-2013-4392**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libsystemd0 | 247.3-6 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2013-4392](https://security-tracker.debian.org/tracker/CVE-2013-4392) |\n"
```

```
}
```

```
},
```

```
{
```

```
"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2013-4392_deb_libudev1_247.3-6",
```

```
"shortDescription": {
```

```
"text": "CVE-2013-4392 Negligible vulnerability for libudev1 package"
```

```
},
```

```

    "fullDescription": {
      "text": "Version 247.3-6 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2013-4392\nSeverity: Negligible\nPackage: libudev1\nVersion: 247.3-6\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2013-4392](https://security-tracker.debian.org/tracker/CVE-2013-4392)",
      "markdown": "***Vulnerability CVE-2013-4392**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libudev1 | 247.3-6 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2013-4392](https://security-tracker.debian.org/tracker/CVE-2013-4392)|\n"
    }
  },
  {
    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2016-2781_deb_coreutils_8.32-4+b1",
    "shortDescription": {
      "text": "CVE-2016-2781 Low vulnerability for coreutils package"
    },
    "fullDescription": {
      "text": "Version 8.32-4+b1 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2016-2781\nSeverity: Low\nPackage: coreutils\nVersion: 8.32-4+b1\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2016-2781](https://security-tracker.debian.org/tracker/CVE-2016-2781)",
      "markdown": "***Vulnerability CVE-2016-2781**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Low | coreutils | 8.32-4+b1 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2016-2781](https://security-tracker.debian.org/tracker/CVE-2016-2781)|\n"
    }
  }
}

```



```

    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2017-11164_deb_libpcre3_2:8.39-13",
    "shortDescription": {
      "text": "CVE-2017-11164 Negligible vulnerability for libpcre3 package"
    },
    "fullDescription": {
      "text": "Version 2:8.39-13 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2017-11164\nSeverity: Negligible\nPackage: libpcre3\nVersion: 2:8.39-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2017-11164](https://security-tracker.debian.org/tracker/CVE-2017-11164)",
      "markdown": "***Vulnerability CVE-2017-11164**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libpcre3 | 2:8.39-13 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2017-11164](https://security-tracker.debian.org/tracker/CVE-2017-11164)|\n"
    }
  },
  {
    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2017-16231_deb_libpcre3_2:8.39-13",
    "shortDescription": {
      "text": "CVE-2017-16231 Negligible vulnerability for libpcre3 package"
    },
    "fullDescription": {
      "text": "Version 2:8.39-13 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2017-16231\nSeverity: Negligible\nPackage: libpcre3\nVersion: 2:8.39-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2017-16231](https://security-tracker.debian.org/tracker/CVE-2017-16231)",
      "markdown": "***Vulnerability CVE-2017-16231**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |"
    }
  }
}

```

|\n|Negligible|libpcre3|2:8.39-13|none|deb|/var/lib/dpkg/status|unknown|[CVE-2017-16231](https://security-tracker.debian.org/tracker/CVE-2017-16231)|\n"

}

},

{

"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2017-18018_deb_coreutils_8.32-4+b1",

"shortDescription": {

"text": "CVE-2017-18018 Negligible vulnerability for coreutils package"

},

"fullDescription": {

"text": "Version 8.32-4+b1 is affected with no fixes reported yet."

},

"help": {

"text": "Vulnerability CVE-2017-18018\nSeverity: Negligible\nPackage: coreutils\nVersion: 8.32-4+b1\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2017-18018](https://security-tracker.debian.org/tracker/CVE-2017-18018)",

"markdown": "***Vulnerability CVE-2017-18018**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n|\n|Negligible|coreutils|8.32-4+b1|none|deb|/var/lib/dpkg/status|unknown|[CVE-2017-18018](https://security-tracker.debian.org/tracker/CVE-2017-18018)|\n"

}

},

{

"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2017-7245_deb_libpcre3_2:8.39-13",

"shortDescription": {

"text": "CVE-2017-7245 Negligible vulnerability for libpcre3 package"

},

"fullDescription": {

"text": "Version 2:8.39-13 is affected with no fixes reported yet."

},

"help": {

```
"text": "Vulnerability CVE-2017-7245\nSeverity: Negligible\nPackage: libpcre3\nVersion: 2:8.39-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2017-7245](https://security-tracker.debian.org/tracker/CVE-2017-7245)",
```

```
"markdown": "***Vulnerability CVE-2017-7245**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libpcre3 | 2:8.39-13 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2017-7245](https://security-tracker.debian.org/tracker/CVE-2017-7245) |\n"
```

```
}
```

```
},
```

```
{
```

```
"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2017-7246_deb_libpcre3_2:8.39-13",
```

```
"shortDescription": {
```

```
"text": "CVE-2017-7246 Negligible vulnerability for libpcre3 package"
```

```
},
```

```
"fullDescription": {
```

```
"text": "Version 2:8.39-13 is affected with no fixes reported yet."
```

```
},
```

```
"help": {
```

```
"text": "Vulnerability CVE-2017-7246\nSeverity: Negligible\nPackage: libpcre3\nVersion: 2:8.39-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2017-7246](https://security-tracker.debian.org/tracker/CVE-2017-7246)",
```

```
"markdown": "***Vulnerability CVE-2017-7246**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libpcre3 | 2:8.39-13 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2017-7246](https://security-tracker.debian.org/tracker/CVE-2017-7246) |\n"
```

```
}
```

```
},
```

```
{
```

```
"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2018-20796_deb_libc-bin_2.31-13",
```

```
"shortDescription": {
```

```
"text": "CVE-2018-20796 Negligible vulnerability for libc-bin package"
```

```
},
```

```

    "fullDescription": {
      "text": "Version 2.31-13 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2018-20796\nSeverity: Negligible\nPackage: libc-bin\nVersion: 2.31-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2018-20796](https://security-tracker.debian.org/tracker/CVE-2018-20796)",
      "markdown": "***Vulnerability CVE-2018-20796**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libc-bin | 2.31-13 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2018-20796](https://security-tracker.debian.org/tracker/CVE-2018-20796) |\n"
    }
  },
  {
    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2018-20796_deb_libc6_2.31-13",
    "shortDescription": {
      "text": "CVE-2018-20796 Negligible vulnerability for libc6 package"
    },
    "fullDescription": {
      "text": "Version 2.31-13 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2018-20796\nSeverity: Negligible\nPackage: libc6\nVersion: 2.31-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2018-20796](https://security-tracker.debian.org/tracker/CVE-2018-20796)",
      "markdown": "***Vulnerability CVE-2018-20796**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libc6 | 2.31-13 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2018-20796](https://security-tracker.debian.org/tracker/CVE-2018-20796) |\n"
    }
  }
}

```

"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2018-5709_deb_libgssapi-krb5-2_1.18.3-6",

"shortDescription": {

"text": "CVE-2018-5709 Negligible vulnerability for libgssapi-krb5-2 package"

},

"fullDescription": {

"text": "Version 1.18.3-6 is affected with no fixes reported yet."

},

"help": {

"text": "Vulnerability CVE-2018-5709\nSeverity: Negligible\nPackage: libgssapi-krb5-2\nVersion: 1.18.3-6\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2018-5709](https://security-tracker.debian.org/tracker/CVE-2018-5709)",

"markdown": "***Vulnerability CVE-2018-5709**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libgssapi-krb5-2 | 1.18.3-6 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2018-5709](https://security-tracker.debian.org/tracker/CVE-2018-5709) |\n"

}

},

{

"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2018-5709_deb_libk5crypto3_1.18.3-6",

"shortDescription": {

"text": "CVE-2018-5709 Negligible vulnerability for libk5crypto3 package"

},

"fullDescription": {

"text": "Version 1.18.3-6 is affected with no fixes reported yet."

},

"help": {

"text": "Vulnerability CVE-2018-5709\nSeverity: Negligible\nPackage: libk5crypto3\nVersion: 1.18.3-6\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2018-5709](https://security-tracker.debian.org/tracker/CVE-2018-5709)",

"markdown": "***Vulnerability CVE-2018-5709**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n"

|\n|Negligible|libk5crypto3|1.18.3-6|none|deb|/var/lib/dpkg/status|unknown|[CVE-2018-5709](https://security-tracker.debian.org/tracker/CVE-2018-5709)|\n"

}

},

{

"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2018-5709_deb_libkrb5-3_1.18.3-6",

"shortDescription": {

"text": "CVE-2018-5709 Negligible vulnerability for libkrb5-3 package"

},

"fullDescription": {

"text": "Version 1.18.3-6 is affected with no fixes reported yet."

},

"help": {

"text": "Vulnerability CVE-2018-5709\nSeverity: Negligible\nPackage: libkrb5-3\nVersion: 1.18.3-6\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2018-5709](https://security-tracker.debian.org/tracker/CVE-2018-5709)",

"markdown": "***Vulnerability CVE-2018-5709**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n|\n|Negligible|libkrb5-3|1.18.3-6|none|deb|/var/lib/dpkg/status|unknown|[CVE-2018-5709](https://security-tracker.debian.org/tracker/CVE-2018-5709)|\n"

}

},

{

"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2018-5709_deb_libkrb5support0_1.18.3-6",

"shortDescription": {

"text": "CVE-2018-5709 Negligible vulnerability for libkrb5support0 package"

},

"fullDescription": {

"text": "Version 1.18.3-6 is affected with no fixes reported yet."

},

```

    "help": {
        "text": "Vulnerability CVE-2018-5709\nSeverity: Negligible\nPackage:
libkrb5support0\nVersion: 1.18.3-6\nFix Version: none\nType: deb\nLocation:
/var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2018-5709](https://security-
tracker.debian.org/tracker/CVE-2018-5709)",
        "markdown": "***Vulnerability CVE-2018-5709**\n| Severity | Package | Version | Fix Version |
Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- | ---
|\n| Negligible | libkrb5support0 | 1.18.3-6 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2018-
5709](https://security-tracker.debian.org/tracker/CVE-2018-5709) |\n"
    }
},
{
    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2018-6829_deb_libcrypt20_1.8.7-6",
    "shortDescription": {
        "text": "CVE-2018-6829 Negligible vulnerability for libcrypt20 package"
    },
    "fullDescription": {
        "text": "Version 1.8.7-6 is affected with no fixes reported yet."
    },
    "help": {
        "text": "Vulnerability CVE-2018-6829\nSeverity: Negligible\nPackage: libcrypt20\nVersion:
1.8.7-6\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace:
unknown\nLink: [CVE-2018-6829](https://security-tracker.debian.org/tracker/CVE-2018-6829)",
        "markdown": "***Vulnerability CVE-2018-6829**\n| Severity | Package | Version | Fix Version |
Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- | ---
|\n| Negligible | libcrypt20 | 1.8.7-6 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2018-
6829](https://security-tracker.debian.org/tracker/CVE-2018-6829) |\n"
    }
},
{
    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-1010022_deb_libc-bin_2.31-13",
    "shortDescription": {
        "text": "CVE-2019-1010022 Negligible vulnerability for libc-bin package"
    }
}

```

```

    },
    "fullDescription": {
      "text": "Version 2.31-13 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2019-1010022\nSeverity: Negligible\nPackage: libc-bin\nVersion: 2.31-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2019-1010022](https://security-tracker.debian.org/tracker/CVE-2019-1010022)",
      "markdown": "***Vulnerability CVE-2019-1010022**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libc-bin | 2.31-13 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2019-1010022](https://security-tracker.debian.org/tracker/CVE-2019-1010022)|\n"
    }
  },
  {
    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-1010022_deb_libc6_2.31-13",
    "shortDescription": {
      "text": "CVE-2019-1010022 Negligible vulnerability for libc6 package"
    },
    "fullDescription": {
      "text": "Version 2.31-13 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2019-1010022\nSeverity: Negligible\nPackage: libc6\nVersion: 2.31-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2019-1010022](https://security-tracker.debian.org/tracker/CVE-2019-1010022)",
      "markdown": "***Vulnerability CVE-2019-1010022**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libc6 | 2.31-13 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2019-1010022](https://security-tracker.debian.org/tracker/CVE-2019-1010022)|\n"
    }
  },

```



```

{
  "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-1010023_deb_libc-bin_2.31-13",
  "shortDescription": {
    "text": "CVE-2019-1010023 Negligible vulnerability for libc-bin package"
  },
  "fullDescription": {
    "text": "Version 2.31-13 is affected with no fixes reported yet."
  },
  "help": {
    "text": "Vulnerability CVE-2019-1010023\nSeverity: Negligible\nPackage: libc-bin\nVersion: 2.31-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2019-1010023](https://security-tracker.debian.org/tracker/CVE-2019-1010023)",
    "markdown": "***Vulnerability CVE-2019-1010023**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libc-bin | 2.31-13 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2019-1010023](https://security-tracker.debian.org/tracker/CVE-2019-1010023)|\n"
  }
},
{
  "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-1010023_deb_libc6_2.31-13",
  "shortDescription": {
    "text": "CVE-2019-1010023 Negligible vulnerability for libc6 package"
  },
  "fullDescription": {
    "text": "Version 2.31-13 is affected with no fixes reported yet."
  },
  "help": {
    "text": "Vulnerability CVE-2019-1010023\nSeverity: Negligible\nPackage: libc6\nVersion: 2.31-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2019-1010023](https://security-tracker.debian.org/tracker/CVE-2019-1010023)",
    "markdown": "***Vulnerability CVE-2019-1010023**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |"
  }
}

```

```
|\n|Negligible|libc6|2.31-13|none|deb|/var/lib/dpkg/status|unknown|[CVE-2019-1010023](https://security-tracker.debian.org/tracker/CVE-2019-1010023)|\n"
```

```
}
```

```
},
```

```
{
```

```
"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-1010024_deb_libc-bin_2.31-13",
```

```
"shortDescription": {
```

```
"text": "CVE-2019-1010024 Negligible vulnerability for libc-bin package"
```

```
},
```

```
"fullDescription": {
```

```
"text": "Version 2.31-13 is affected with no fixes reported yet."
```

```
},
```

```
"help": {
```

```
"text": "Vulnerability CVE-2019-1010024\nSeverity: Negligible\nPackage: libc-bin\nVersion: 2.31-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2019-1010024](https://security-tracker.debian.org/tracker/CVE-2019-1010024)",
```

```
"markdown": "***Vulnerability CVE-2019-1010024**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n|\n|Negligible|libc-bin|2.31-13|none|deb|/var/lib/dpkg/status|unknown|[CVE-2019-1010024](https://security-tracker.debian.org/tracker/CVE-2019-1010024)|\n"
```

```
}
```

```
},
```

```
{
```

```
"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-1010024_deb_libc6_2.31-13",
```

```
"shortDescription": {
```

```
"text": "CVE-2019-1010024 Negligible vulnerability for libc6 package"
```

```
},
```

```
"fullDescription": {
```

```
"text": "Version 2.31-13 is affected with no fixes reported yet."
```

```
},
```

```
"help": {
```

```
"text": "Vulnerability CVE-2019-1010024\nSeverity: Negligible\nPackage: libc6\nVersion: 2.31-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2019-1010024](https://security-tracker.debian.org/tracker/CVE-2019-1010024)",
```

```
"markdown": "***Vulnerability CVE-2019-1010024**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libc6 | 2.31-13 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2019-1010024](https://security-tracker.debian.org/tracker/CVE-2019-1010024)|\n"
```

```
}
```

```
},
```

```
{
```

```
"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-1010025_deb_libc-bin_2.31-13",
```

```
"shortDescription": {
```

```
"text": "CVE-2019-1010025 Negligible vulnerability for libc-bin package"
```

```
},
```

```
"fullDescription": {
```

```
"text": "Version 2.31-13 is affected with no fixes reported yet."
```

```
},
```

```
"help": {
```

```
"text": "Vulnerability CVE-2019-1010025\nSeverity: Negligible\nPackage: libc-bin\nVersion: 2.31-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2019-1010025](https://security-tracker.debian.org/tracker/CVE-2019-1010025)",
```

```
"markdown": "***Vulnerability CVE-2019-1010025**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libc-bin | 2.31-13 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2019-1010025](https://security-tracker.debian.org/tracker/CVE-2019-1010025)|\n"
```

```
}
```

```
},
```

```
{
```

```
"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-1010025_deb_libc6_2.31-13",
```

```
"shortDescription": {
```

```
"text": "CVE-2019-1010025 Negligible vulnerability for libc6 package"
```

```
},
```

```

    "fullDescription": {
      "text": "Version 2.31-13 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2019-1010025\nSeverity: Negligible\nPackage: libc6\nVersion: 2.31-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2019-1010025](https://security-tracker.debian.org/tracker/CVE-2019-1010025)",
      "markdown": "***Vulnerability CVE-2019-1010025**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libc6 | 2.31-13 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2019-1010025](https://security-tracker.debian.org/tracker/CVE-2019-1010025)|\n"
    }
  },
  {
    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-19882_deb_login_1:4.8.1-1",
    "shortDescription": {
      "text": "CVE-2019-19882 Negligible vulnerability for login package"
    },
    "fullDescription": {
      "text": "Version 1:4.8.1-1 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2019-19882\nSeverity: Negligible\nPackage: login\nVersion: 1:4.8.1-1\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2019-19882](https://security-tracker.debian.org/tracker/CVE-2019-19882)",
      "markdown": "***Vulnerability CVE-2019-19882**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | login | 1:4.8.1-1 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2019-19882](https://security-tracker.debian.org/tracker/CVE-2019-19882)|\n"
    }
  }
}

```

```

    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-19882_deb_passwd_1:4.8.1-1",
    "shortDescription": {
      "text": "CVE-2019-19882 Negligible vulnerability for passwd package"
    },
    "fullDescription": {
      "text": "Version 1:4.8.1-1 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2019-19882\nSeverity: Negligible\nPackage: passwd\nVersion: 1:4.8.1-1\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2019-19882](https://security-tracker.debian.org/tracker/CVE-2019-19882)",
      "markdown": "***Vulnerability CVE-2019-19882**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | passwd | 1:4.8.1-1 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2019-19882](https://security-tracker.debian.org/tracker/CVE-2019-19882) |\n"
    }
  },
  {
    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-20838_deb_libpcre3_2:8.39-13",
    "shortDescription": {
      "text": "CVE-2019-20838 Negligible vulnerability for libpcre3 package"
    },
    "fullDescription": {
      "text": "Version 2:8.39-13 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2019-20838\nSeverity: Negligible\nPackage: libpcre3\nVersion: 2:8.39-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2019-20838](https://security-tracker.debian.org/tracker/CVE-2019-20838)",
      "markdown": "***Vulnerability CVE-2019-20838**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |"
    }
  }
}

```

|\n|Negligible|libpcre3|2:8.39-13|none|deb|/var/lib/dpkg/status|unknown|[CVE-2019-20838](https://security-tracker.debian.org/tracker/CVE-2019-20838)|\n"

}

},

{

"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-9192_deb_libc-bin_2.31-13",

"shortDescription": {

"text": "CVE-2019-9192 Negligible vulnerability for libc-bin package"

},

"fullDescription": {

"text": "Version 2.31-13 is affected with no fixes reported yet."

},

"help": {

"text": "Vulnerability CVE-2019-9192\nSeverity: Negligible\nPackage: libc-bin\nVersion: 2.31-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2019-9192](https://security-tracker.debian.org/tracker/CVE-2019-9192)",

"markdown": "***Vulnerability CVE-2019-9192**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libc-bin | 2.31-13 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2019-9192](https://security-tracker.debian.org/tracker/CVE-2019-9192) |\n"

}

},

{

"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-9192_deb_libc6_2.31-13",

"shortDescription": {

"text": "CVE-2019-9192 Negligible vulnerability for libc6 package"

},

"fullDescription": {

"text": "Version 2.31-13 is affected with no fixes reported yet."

},

"help": {

"text": "Vulnerability CVE-2019-9192\nSeverity: Negligible\nPackage: libc6\nVersion: 2.31-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2019-9192](https://security-tracker.debian.org/tracker/CVE-2019-9192)",

"markdown": "***Vulnerability CVE-2019-9192**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libc6 | 2.31-13 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2019-9192](https://security-tracker.debian.org/tracker/CVE-2019-9192) |\n"

}

},

{

"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2020-13529_deb_libsystemd0_247.3-6",

"shortDescription": {

"text": "CVE-2020-13529 Negligible vulnerability for libsystemd0 package"

},

"fullDescription": {

"text": "Version 247.3-6 is affected with no fixes reported yet."

},

"help": {

"text": "Vulnerability CVE-2020-13529\nSeverity: Negligible\nPackage: libsystemd0\nVersion: 247.3-6\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2020-13529](https://security-tracker.debian.org/tracker/CVE-2020-13529)",

"markdown": "***Vulnerability CVE-2020-13529**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libsystemd0 | 247.3-6 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2020-13529](https://security-tracker.debian.org/tracker/CVE-2020-13529) |\n"

}

},

{

"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2020-13529_deb_libudev1_247.3-6",

"shortDescription": {

"text": "CVE-2020-13529 Negligible vulnerability for libudev1 package"

},

```

    "fullDescription": {
      "text": "Version 247.3-6 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2020-13529\nSeverity: Negligible\nPackage: libudev1\nVersion: 247.3-6\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2020-13529](https://security-tracker.debian.org/tracker/CVE-2020-13529)",
      "markdown": "***Vulnerability CVE-2020-13529**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libudev1 | 247.3-6 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2020-13529](https://security-tracker.debian.org/tracker/CVE-2020-13529)|\n"
    }
  },
  {
    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-33574_deb_libc-bin_2.31-13",
    "shortDescription": {
      "text": "CVE-2021-33574 Critical vulnerability for libc-bin package"
    },
    "fullDescription": {
      "text": "Version 2.31-13 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2021-33574\nSeverity: Critical\nPackage: libc-bin\nVersion: 2.31-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2021-33574](https://security-tracker.debian.org/tracker/CVE-2021-33574)",
      "markdown": "***Vulnerability CVE-2021-33574**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Critical | libc-bin | 2.31-13 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2021-33574](https://security-tracker.debian.org/tracker/CVE-2021-33574)|\n"
    }
  }
}

```



```

    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-33574_deb_libc6_2.31-13",
    "shortDescription": {
      "text": "CVE-2021-33574 Critical vulnerability for libc6 package"
    },
    "fullDescription": {
      "text": "Version 2.31-13 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2021-33574\nSeverity: Critical\nPackage: libc6\nVersion: 2.31-13\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2021-33574](https://security-tracker.debian.org/tracker/CVE-2021-33574)",
      "markdown": "***Vulnerability CVE-2021-33574**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Critical | libc6 | 2.31-13 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2021-33574](https://security-tracker.debian.org/tracker/CVE-2021-33574) |\n"
    }
  },
  {
    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-36084_deb_libsepol1_3.1-1",
    "shortDescription": {
      "text": "CVE-2021-36084 Low vulnerability for libsepol1 package"
    },
    "fullDescription": {
      "text": "Version 3.1-1 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2021-36084\nSeverity: Low\nPackage: libsepol1\nVersion: 3.1-1\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2021-36084](https://security-tracker.debian.org/tracker/CVE-2021-36084)",
      "markdown": "***Vulnerability CVE-2021-36084**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |"
    }
  }
}

```

```
|\n|Low|libsepol1|3.1-1|none|deb|/var/lib/dpkg/status|unknown|[CVE-2021-36084](https://security-tracker.debian.org/tracker/CVE-2021-36084)|\n"
```

```
}
```

```
},
```

```
{
```

```
"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-36085_deb_libsepol1_3.1-1",
```

```
"shortDescription": {
```

```
"text": "CVE-2021-36085 Low vulnerability for libsepol1 package"
```

```
},
```

```
"fullDescription": {
```

```
"text": "Version 3.1-1 is affected with no fixes reported yet."
```

```
},
```

```
"help": {
```

```
"text": "Vulnerability CVE-2021-36085\nSeverity: Low\nPackage: libsepol1\nVersion: 3.1-1\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2021-36085](https://security-tracker.debian.org/tracker/CVE-2021-36085)",
```

```
"markdown": "***Vulnerability CVE-2021-36085**\n| Severity | Package | Version | Fix Version |\n| Type | Location | Data Namespace | Link |\n|\n|Low|libsepol1|3.1-1|none|deb|/var/lib/dpkg/status|unknown|[CVE-2021-36085](https://security-tracker.debian.org/tracker/CVE-2021-36085)|\n"
```

```
}
```

```
},
```

```
{
```

```
"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-36086_deb_libsepol1_3.1-1",
```

```
"shortDescription": {
```

```
"text": "CVE-2021-36086 Low vulnerability for libsepol1 package"
```

```
},
```

```
"fullDescription": {
```

```
"text": "Version 3.1-1 is affected with no fixes reported yet."
```

```
},
```

```
"help": {
```

```
"text": "Vulnerability CVE-2021-36086\nSeverity: Low\nPackage: libsepol1\nVersion: 3.1-1\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2021-36086](https://security-tracker.debian.org/tracker/CVE-2021-36086)",
```

```
"markdown": "***Vulnerability CVE-2021-36086**\n| Severity | Package | Version | Fix Version |\n| Type | Location | Data Namespace | Link |\n| Low | libsepol1 | 3.1-1 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2021-36086](https://security-tracker.debian.org/tracker/CVE-2021-36086)|\n"
```

```
}
```

```
},
```

```
{
```

```
"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-36087_deb_libsepol1_3.1-1",
```

```
"shortDescription": {
```

```
"text": "CVE-2021-36087 Low vulnerability for libsepol1 package"
```

```
},
```

```
"fullDescription": {
```

```
"text": "Version 3.1-1 is affected with no fixes reported yet."
```

```
},
```

```
"help": {
```

```
"text": "Vulnerability CVE-2021-36087\nSeverity: Low\nPackage: libsepol1\nVersion: 3.1-1\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2021-36087](https://security-tracker.debian.org/tracker/CVE-2021-36087)",
```

```
"markdown": "***Vulnerability CVE-2021-36087**\n| Severity | Package | Version | Fix Version |\n| Type | Location | Data Namespace | Link |\n| Low | libsepol1 | 3.1-1 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2021-36087](https://security-tracker.debian.org/tracker/CVE-2021-36087)|\n"
```

```
}
```

```
},
```

```
{
```

```
"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-36690_deb_libsqlite3-0_3.34.1-3",
```

```
"shortDescription": {
```

```
"text": "CVE-2021-36690 Negligible vulnerability for libsqlite3-0 package"
```

```
},
```

```

    "fullDescription": {
      "text": "Version 3.34.1-3 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2021-36690\nSeverity: Negligible\nPackage: libsqlite3-0\nVersion: 3.34.1-3\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2021-36690](https://security-tracker.debian.org/tracker/CVE-2021-36690)",
      "markdown": "***Vulnerability CVE-2021-36690**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libsqlite3-0 | 3.34.1-3 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2021-36690](https://security-tracker.debian.org/tracker/CVE-2021-36690) |\n"
    }
  },
  {
    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-37750_deb_libgssapi-krb5-2_1.18.3-6",
    "shortDescription": {
      "text": "CVE-2021-37750 Medium vulnerability for libgssapi-krb5-2 package"
    },
    "fullDescription": {
      "text": "Version 1.18.3-6 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2021-37750\nSeverity: Medium\nPackage: libgssapi-krb5-2\nVersion: 1.18.3-6\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2021-37750](https://security-tracker.debian.org/tracker/CVE-2021-37750)",
      "markdown": "***Vulnerability CVE-2021-37750**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Medium | libgssapi-krb5-2 | 1.18.3-6 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2021-37750](https://security-tracker.debian.org/tracker/CVE-2021-37750) |\n"
    }
  }
}

```

```

6",
  "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-37750_deb_libk5crypto3_1.18.3-6",
  "shortDescription": {
    "text": "CVE-2021-37750 Medium vulnerability for libk5crypto3 package"
  },
  "fullDescription": {
    "text": "Version 1.18.3-6 is affected with no fixes reported yet."
  },
  "help": {
    "text": "Vulnerability CVE-2021-37750\nSeverity: Medium\nPackage: libk5crypto3\nVersion: 1.18.3-6\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2021-37750](https://security-tracker.debian.org/tracker/CVE-2021-37750)",
    "markdown": "***Vulnerability CVE-2021-37750**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Medium | libk5crypto3 | 1.18.3-6 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2021-37750](https://security-tracker.debian.org/tracker/CVE-2021-37750) |\n"
  }
},
{
  "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-37750_deb_libkrb5-3_1.18.3-6",
  "shortDescription": {
    "text": "CVE-2021-37750 Medium vulnerability for libkrb5-3 package"
  },
  "fullDescription": {
    "text": "Version 1.18.3-6 is affected with no fixes reported yet."
  },
  "help": {
    "text": "Vulnerability CVE-2021-37750\nSeverity: Medium\nPackage: libkrb5-3\nVersion: 1.18.3-6\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2021-37750](https://security-tracker.debian.org/tracker/CVE-2021-37750)",
    "markdown": "***Vulnerability CVE-2021-37750**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Medium | libkrb5-3 | 1.18.3-6 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2021-37750](https://security-tracker.debian.org/tracker/CVE-2021-37750) |\n"
  }
}

```

3|1.18.3-6|none|deb|/var/lib/dpkg/status|unknown|[CVE-2021-37750](https://security-tracker.debian.org/tracker/CVE-2021-37750)|\n"

}

},

{

"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-37750_deb_libkrb5support0_1.18.3-6",

"shortDescription": {

"text": "CVE-2021-37750 Medium vulnerability for libkrb5support0 package"

},

"fullDescription": {

"text": "Version 1.18.3-6 is affected with no fixes reported yet."

},

"help": {

"text": "Vulnerability CVE-2021-37750\nSeverity: Medium\nPackage: libkrb5support0\nVersion: 1.18.3-6\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2021-37750](https://security-tracker.debian.org/tracker/CVE-2021-37750)",

"markdown": "***Vulnerability CVE-2021-37750**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Medium | libkrb5support0 | 1.18.3-6 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2021-37750](https://security-tracker.debian.org/tracker/CVE-2021-37750) |\n"

}

},

{

"id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-39537_deb_libncursesw6_6.2+20201114-2",

"shortDescription": {

"text": "CVE-2021-39537 Negligible vulnerability for libncursesw6 package"

},

"fullDescription": {

"text": "Version 6.2+20201114-2 is affected with no fixes reported yet."

```

    },
    "help": {
        "text": "Vulnerability CVE-2021-39537\nSeverity: Negligible\nPackage: libncursesw6\nVersion: 6.2+20201114-2\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2021-39537](https://security-tracker.debian.org/tracker/CVE-2021-39537)",
        "markdown": "***Vulnerability CVE-2021-39537**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libncursesw6 | 6.2+20201114-2 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2021-39537](https://security-tracker.debian.org/tracker/CVE-2021-39537) |\n"
    }
},
{
    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-39537_deb_libtinfo6_6.2+20201114-2",
    "shortDescription": {
        "text": "CVE-2021-39537 Negligible vulnerability for libtinfo6 package"
    },
    "fullDescription": {
        "text": "Version 6.2+20201114-2 is affected with no fixes reported yet."
    },
    "help": {
        "text": "Vulnerability CVE-2021-39537\nSeverity: Negligible\nPackage: libtinfo6\nVersion: 6.2+20201114-2\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2021-39537](https://security-tracker.debian.org/tracker/CVE-2021-39537)",
        "markdown": "***Vulnerability CVE-2021-39537**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | libtinfo6 | 6.2+20201114-2 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2021-39537](https://security-tracker.debian.org/tracker/CVE-2021-39537) |\n"
    }
},
{
    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-39537_deb_ncurses-base_6.2+20201114-2",

```

```

"shortDescription": {
  "text": "CVE-2021-39537 Negligible vulnerability for ncurses-base package"
},
"fullDescription": {
  "text": "Version 6.2+20201114-2 is affected with no fixes reported yet."
},
"help": {
  "text": "Vulnerability CVE-2021-39537\nSeverity: Negligible\nPackage: ncurses-base\nVersion: 6.2+20201114-2\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2021-39537](https://security-tracker.debian.org/tracker/CVE-2021-39537)",
  "markdown": "***Vulnerability CVE-2021-39537**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | ncurses-base | 6.2+20201114-2 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2021-39537](https://security-tracker.debian.org/tracker/CVE-2021-39537) |\n"
}
},
{
  "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-39537_deb_ncurses-bin_6.2+20201114-2",
  "shortDescription": {
    "text": "CVE-2021-39537 Negligible vulnerability for ncurses-bin package"
  },
  "fullDescription": {
    "text": "Version 6.2+20201114-2 is affected with no fixes reported yet."
  },
  "help": {
    "text": "Vulnerability CVE-2021-39537\nSeverity: Negligible\nPackage: ncurses-bin\nVersion: 6.2+20201114-2\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2021-39537](https://security-tracker.debian.org/tracker/CVE-2021-39537)",
    "markdown": "***Vulnerability CVE-2021-39537**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| Negligible | ncurses-bin | 6.2+20201114-2 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2021-39537](https://security-tracker.debian.org/tracker/CVE-2021-39537) |\n"
  }
}

```



```

    }
  },
  {
    "id": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-40528_deb_libcrypt20_1.8.7-6",
    "shortDescription": {
      "text": "CVE-2021-40528 Medium vulnerability for libcrypt20 package"
    },
    "fullDescription": {
      "text": "Version 1.8.7-6 is affected with no fixes reported yet."
    },
    "help": {
      "text": "Vulnerability CVE-2021-40528\nSeverity: Medium\nPackage: libcrypt20\nVersion: 1.8.7-6\nFix Version: none\nType: deb\nLocation: /var/lib/dpkg/status\nData Namespace: unknown\nLink: [CVE-2021-40528](https://security-tracker.debian.org/tracker/CVE-2021-40528)",
      "markdown": "***Vulnerability CVE-2021-40528**\n| Severity | Package | Version | Fix Version | Type | Location | Data Namespace | Link |\n| --- | --- | --- | --- | --- | --- | --- | --- |\n| \n| Medium | libcrypt20 | 1.8.7-6 | none | deb | /var/lib/dpkg/status | unknown | [CVE-2021-40528](https://security-tracker.debian.org/tracker/CVE-2021-40528)|\n"
    }
  }
]
},
"logicalLocations": [
  {
    "name": "dockerfile",
    "fullyQualified_name": "dockerfile",
    "kind": "namespace"
  }
],

```

```
"results": [  
  {  
    "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2004-0971_deb_libgssapi-krb5-  
2_1.18.3-6",  
    "ruleIndex": 0,  
    "level": "warning",  
    "message": {  
      "text": "The path /var/lib/dpkg/status reports libgssapi-krb5-2 at version 1.18.3-6 which is a  
vulnerable (deb) package installed in the container",  
      "id": "default"  
    },  
    "analysisTarget": {  
      "uri": "/var/lib/dpkg/status"  
    },  
    "locations": [  
      {  
        "physicalLocation": {  
          "artifactLocation": {  
            "uri": "/var/lib/dpkg/status"  
          },  
          "region": {  
            "startLine": 1,  
            "startColumn": 1,  
            "endLine": 1,  
            "endColumn": 1,  
            "byteOffset": 1,  
            "byteLength": 1  
          }  
        },  
      ],  
    ],  
  },  
]
```

```
"logicalLocations": [  
  {  
    "fullyQualifiedName": "dockerfile"  
  }  
]  
}  
],  
"suppressions": [  
  {  
    "kind": "external"  
  }  
],  
"baselineState": "unchanged"  
},  
{  
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2004-0971_deb_libk5crypto3_1.18.3-  
6",  
  "ruleIndex": 0,  
  "level": "warning",  
  "message": {  
    "text": "The path /var/lib/dpkg/status reports libk5crypto3 at version 1.18.3-6 which is a  
vulnerable (deb) package installed in the container",  
    "id": "default"  
  },  
  "analysisTarget": {  
    "uri": "/var/lib/dpkg/status"  
  },  
  "locations": [  
    {
```

```
"physicalLocation": {
  "artifactLocation": {
    "uri": "/var/lib/dpkg/status"
  },
  "region": {
    "startLine": 1,
    "startColumn": 1,
    "endLine": 1,
    "endColumn": 1,
    "byteOffset": 1,
    "byteLength": 1
  }
},
"logicalLocations": [
  {
    "fullyQualifiedName": "dockerfile"
  }
]
},
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2004-0971_deb_libkrb5-3_1.18.3-6",
```

```
"ruleIndex": 0,

"level": "warning",

"message": {

  "text": "The path /var/lib/dpkg/status reports libkrb5-3 at version 1.18.3-6 which is a vulnerable
(deb) package installed in the container",

  "id": "default"

},

"analysisTarget": {

  "uri": "/var/lib/dpkg/status"

},

"locations": [

{

  "physicalLocation": {

    "artifactLocation": {

      "uri": "/var/lib/dpkg/status"

    },

    "region": {

      "startLine": 1,

      "startColumn": 1,

      "endLine": 1,

      "endColumn": 1,

      "byteOffset": 1,

      "byteLength": 1

    }

  },

  "logicalLocations": [

    {

      "fullyQualifiedName": "dockerfile"

    }

  ]

}
```

```
    ]
  }
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2004-0971_deb_libkrb5support0_1.18.3-6",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libkrb5support0 at version 1.18.3-6 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        }
      },
    },
  ],
}
```

```
"region": {
  "startLine": 1,
  "startColumn": 1,
  "endLine": 1,
  "endColumn": 1,
  "byteOffset": 1,
  "byteLength": 1
},
"logicalLocations": [
  {
    "fullyQualifiedName": "dockerfile"
  }
]
},
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2005-2541_deb_tar_1.34+dfsg-1",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
```

"text": "The path /var/lib/dpkg/status reports tar at version 1.34+dfsg-1 which is a vulnerable (deb) package installed in the container",

"id": "default"

},

"analysisTarget": {

"uri": "/var/lib/dpkg/status"

},

"locations": [

{

"physicalLocation": {

"artifactLocation": {

"uri": "/var/lib/dpkg/status"

},

"region": {

"startLine": 1,

"startColumn": 1,

"endLine": 1,

"endColumn": 1,

"byteOffset": 1,

"byteLength": 1

}

},

"logicalLocations": [

{

"fullyQualifiedName": "dockerfile"

}

]

}

],


```
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2007-5686_deb_login_1:4.8.1-1",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports login at version 1:4.8.1-1 which is a vulnerable
(deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        },
        "region": {
          "startLine": 1,
          "startColumn": 1,
          "endLine": 1,
```

```
        "endColumn": 1,
        "byteOffset": 1,
        "byteLength": 1
    }
},
"logicalLocations": [
    {
        "fullyQualifiedName": "dockerfile"
    }
]
},
"suppressions": [
    {
        "kind": "external"
    }
],
"baselineState": "unchanged"
},
{
    "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2007-5686_deb_passwd_1:4.8.1-1",
    "ruleIndex": 0,
    "level": "warning",
    "message": {
        "text": "The path /var/lib/dpkg/status reports passwd at version 1:4.8.1-1 which is a vulnerable (deb) package installed in the container",
        "id": "default"
    }
},
"analysisTarget": {
```

```
"uri": "/var/lib/dpkg/status"
},
"locations": [
  {
    "physicalLocation": {
      "artifactLocation": {
        "uri": "/var/lib/dpkg/status"
      },
      "region": {
        "startLine": 1,
        "startColumn": 1,
        "endLine": 1,
        "endColumn": 1,
        "byteOffset": 1,
        "byteLength": 1
      }
    },
    "logicalLocations": [
      {
        "fullyQualifiedName": "dockerfile"
      }
    ]
  }
],
"suppressions": [
  {
    "kind": "external"
  }
],
```

```
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2007-6755_deb_libssl1.1_1.1.1k-1+deb11u1",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libssl1.1 at version 1.1.1k-1+deb11u1 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        },
        "region": {
          "startLine": 1,
          "startColumn": 1,
          "endLine": 1,
          "endColumn": 1,
          "byteOffset": 1,
          "byteLength": 1
        }
      }
    }
  ]
}
```

```
    },
    "logicalLocations": [
      {
        "fullyQualifiedName": "dockerfile"
      }
    ]
  },
  ],
  "suppressions": [
    {
      "kind": "external"
    }
  ],
  ],
  "baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2007-6755_deb_openssl_1.1.1k-1+deb11u1",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports openssl at version 1.1.1k-1+deb11u1 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  ],
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  ],
  "locations": [
```

```
{
  "physicalLocation": {
    "artifactLocation": {
      "uri": "/var/lib/dpkg/status"
    },
    "region": {
      "startLine": 1,
      "startColumn": 1,
      "endLine": 1,
      "endColumn": 1,
      "byteOffset": 1,
      "byteLength": 1
    }
  },
  "logicalLocations": [
    {
      "fullyQualifiedName": "dockerfile"
    }
  ]
},
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
```

```
"ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2010-0928_deb_libssl1.1_1.1.1k-1+deb11u1",
"ruleIndex": 0,
"level": "warning",
"message": {
  "text": "The path /var/lib/dpkg/status reports libssl1.1 at version 1.1.1k-1+deb11u1 which is a vulnerable (deb) package installed in the container",
  "id": "default"
},
"analysisTarget": {
  "uri": "/var/lib/dpkg/status"
},
"locations": [
  {
    "physicalLocation": {
      "artifactLocation": {
        "uri": "/var/lib/dpkg/status"
      },
      "region": {
        "startLine": 1,
        "startColumn": 1,
        "endLine": 1,
        "endColumn": 1,
        "byteOffset": 1,
        "byteLength": 1
      }
    },
    "logicalLocations": [
      {
```

```
        "fullyQualifiedName": "dockerfile"
      }
    ]
  },
  ],
  "suppressions": [
    {
      "kind": "external"
    }
  ],
  "baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2010-0928_deb_openssl_1.1.1k-1+deb11u1",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports openssl at version 1.1.1k-1+deb11u1 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
```



```
    "uri": "/var/lib/dpkg/status"
  },
  "region": {
    "startLine": 1,
    "startColumn": 1,
    "endLine": 1,
    "endColumn": 1,
    "byteOffset": 1,
    "byteLength": 1
  }
},
"logicalLocations": [
  {
    "fullyQualifiedName": "dockerfile"
  }
]
},
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2010-4051_deb_libc-bin_2.31-13",
  "ruleIndex": 0,
  "level": "warning",
```

```
"message": {
  "text": "The path /var/lib/dpkg/status reports libc-bin at version 2.31-13 which is a vulnerable
(deb) package installed in the container",
  "id": "default"
},
"analysisTarget": {
  "uri": "/var/lib/dpkg/status"
},
"locations": [
{
  "physicalLocation": {
    "artifactLocation": {
      "uri": "/var/lib/dpkg/status"
    },
    "region": {
      "startLine": 1,
      "startColumn": 1,
      "endLine": 1,
      "endColumn": 1,
      "byteOffset": 1,
      "byteLength": 1
    }
  },
  "logicalLocations": [
    {
      "fullyQualifiedName": "dockerfile"
    }
  ]
}
]
```

```
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2010-4051_deb_libc6_2.31-13",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libc6 at version 2.31-13 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        },
        "region": {
          "startLine": 1,
          "startColumn": 1,
```

```
    "endLine": 1,
    "endColumn": 1,
    "byteOffset": 1,
    "byteLength": 1
  }
},
"logicalLocations": [
  {
    "fullyQualifiedName": "dockerfile"
  }
]
},
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2010-4052_deb_libc-bin_2.31-13",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libc-bin at version 2.31-13 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  }
},
```

```
"analysisTarget": {
  "uri": "/var/lib/dpkg/status"
},
"locations": [
  {
    "physicalLocation": {
      "artifactLocation": {
        "uri": "/var/lib/dpkg/status"
      },
      "region": {
        "startLine": 1,
        "startColumn": 1,
        "endLine": 1,
        "endColumn": 1,
        "byteOffset": 1,
        "byteLength": 1
      }
    },
    "logicalLocations": [
      {
        "fullyQualifiedName": "dockerfile"
      }
    ]
  }
],
"suppressions": [
  {
    "kind": "external"
  }
]
```

```
    ],  
    "baselineState": "unchanged"  
  },  
  {  
    "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2010-4052_deb_libc6_2.31-13",  
    "ruleIndex": 0,  
    "level": "warning",  
    "message": {  
      "text": "The path /var/lib/dpkg/status reports libc6 at version 2.31-13 which is a vulnerable (deb)  
package installed in the container",  
      "id": "default"  
    },  
    "analysisTarget": {  
      "uri": "/var/lib/dpkg/status"  
    },  
    "locations": [  
      {  
        "physicalLocation": {  
          "artifactLocation": {  
            "uri": "/var/lib/dpkg/status"  
          },  
          "region": {  
            "startLine": 1,  
            "startColumn": 1,  
            "endLine": 1,  
            "endColumn": 1,  
            "byteOffset": 1,  
            "byteLength": 1  
          }  
        }  
      ]  
    }  
  }  
}
```

```
    },
    "logicalLocations": [
      {
        "fullyQualifiedName": "dockerfile"
      }
    ]
  }
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2010-4756_deb_libc-bin_2.31-13",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libc-bin at version 2.31-13 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
```

```
"physicalLocation": {
  "artifactLocation": {
    "uri": "/var/lib/dpkg/status"
  },
  "region": {
    "startLine": 1,
    "startColumn": 1,
    "endLine": 1,
    "endColumn": 1,
    "byteOffset": 1,
    "byteLength": 1
  }
},
"logicalLocations": [
  {
    "fullyQualifiedName": "dockerfile"
  }
]
},
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2010-4756_deb_libc6_2.31-13",
```



```
"ruleIndex": 0,
"level": "warning",
"message": {
  "text": "The path /var/lib/dpkg/status reports libc6 at version 2.31-13 which is a vulnerable (deb)
package installed in the container",
  "id": "default"
},
"analysisTarget": {
  "uri": "/var/lib/dpkg/status"
},
"locations": [
  {
    "physicalLocation": {
      "artifactLocation": {
        "uri": "/var/lib/dpkg/status"
      },
      "region": {
        "startLine": 1,
        "startColumn": 1,
        "endLine": 1,
        "endColumn": 1,
        "byteOffset": 1,
        "byteLength": 1
      }
    },
    "logicalLocations": [
      {
        "fullyQualifiedName": "dockerfile"
      }
    ]
  }
]
```

```
    ]
  }
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2011-3374_deb_apt_2.2.4",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports apt at version 2.2.4 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        }
      },
      "region": {
```

```
    "startLine": 1,
    "startColumn": 1,
    "endLine": 1,
    "endColumn": 1,
    "byteOffset": 1,
    "byteLength": 1
  }
},
"logicalLocations": [
  {
    "fullyQualifiedName": "dockerfile"
  }
]
}
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2011-3374_deb_libapt-pkg6.0_2.2.4",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libapt-pkg6.0 at version 2.2.4 which is a vulnerable (deb) package installed in the container",
```

```
"id": "default"
},
"analysisTarget": {
  "uri": "/var/lib/dpkg/status"
},
"locations": [
  {
    "physicalLocation": {
      "artifactLocation": {
        "uri": "/var/lib/dpkg/status"
      },
      "region": {
        "startLine": 1,
        "startColumn": 1,
        "endLine": 1,
        "endColumn": 1,
        "byteOffset": 1,
        "byteLength": 1
      }
    },
    "logicalLocations": [
      {
        "fullyQualifiedName": "dockerfile"
      }
    ]
  }
],
"suppressions": [
  {
```

```
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2011-3389_deb_libgnutls30_3.7.1-5",
  "ruleIndex": 0,
  "level": "error",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libgnutls30 at version 3.7.1-5 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        },
        "region": {
          "startLine": 1,
          "startColumn": 1,
          "endLine": 1,
          "endColumn": 1,
          "byteOffset": 1,

```

```
    "byteLength": 1
  }
},
"logicalLocations": [
  {
    "fullyQualifiedName": "dockerfile"
  }
]
}
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2011-4116_deb_perl-base_5.32.1-4+deb11u1",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports perl-base at version 5.32.1-4+deb11u1 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
```

```
},  
"locations": [  
  {  
    "physicalLocation": {  
      "artifactLocation": {  
        "uri": "/var/lib/dpkg/status"  
      },  
      "region": {  
        "startLine": 1,  
        "startColumn": 1,  
        "endLine": 1,  
        "endColumn": 1,  
        "byteOffset": 1,  
        "byteLength": 1  
      }  
    },  
    "logicalLocations": [  
      {  
        "fullyQualifiedName": "dockerfile"  
      }  
    ]  
  }  
],  
"suppressions": [  
  {  
    "kind": "external"  
  }  
],  
"baselineState": "unchanged"
```

```
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2013-0340_deb_libexpat1_2.2.10-2",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libexpat1 at version 2.2.10-2 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        },
        "region": {
          "startLine": 1,
          "startColumn": 1,
          "endLine": 1,
          "endColumn": 1,
          "byteOffset": 1,
          "byteLength": 1
        }
      }
    }
  ],
  "logicalLocations": [
```



```
{
  "fullyQualifiedNames": ["dockerfile"]
}
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2013-4235_deb_login_1:4.8.1-1",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports login at version 1:4.8.1-1 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
```

```
    "uri": "/var/lib/dpkg/status"
  },
  "region": {
    "startLine": 1,
    "startColumn": 1,
    "endLine": 1,
    "endColumn": 1,
    "byteOffset": 1,
    "byteLength": 1
  }
},
"logicalLocations": [
  {
    "fullyQualifiedName": "dockerfile"
  }
]
},
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2013-4235_deb_passwd_1:4.8.1-1",
  "ruleIndex": 0,
  "level": "warning",
```

```
"message": {
  "text": "The path /var/lib/dpkg/status reports passwd at version 1:4.8.1-1 which is a vulnerable
(deb) package installed in the container",
  "id": "default"
},
"analysisTarget": {
  "uri": "/var/lib/dpkg/status"
},
"locations": [
{
  "physicalLocation": {
    "artifactLocation": {
      "uri": "/var/lib/dpkg/status"
    },
    "region": {
      "startLine": 1,
      "startColumn": 1,
      "endLine": 1,
      "endColumn": 1,
      "byteOffset": 1,
      "byteLength": 1
    }
  },
  "logicalLocations": [
    {
      "fullyQualifiedName": "dockerfile"
    }
  ]
}
]
```

```
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2013-4392_deb_libsystemd0_247.3-6",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libsystemd0 at version 247.3-6 which is a
vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        },
        "region": {
          "startLine": 1,
          "startColumn": 1,
```

```
    "endLine": 1,
    "endColumn": 1,
    "byteOffset": 1,
    "byteLength": 1
  }
},
"logicalLocations": [
  {
    "fullyQualifiedName": "dockerfile"
  }
]
},
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2013-4392_deb_libudev1_247.3-6",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libudev1 at version 247.3-6 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  }
},
```

```
"analysisTarget": {
  "uri": "/var/lib/dpkg/status"
},
"locations": [
  {
    "physicalLocation": {
      "artifactLocation": {
        "uri": "/var/lib/dpkg/status"
      },
      "region": {
        "startLine": 1,
        "startColumn": 1,
        "endLine": 1,
        "endColumn": 1,
        "byteOffset": 1,
        "byteLength": 1
      }
    },
    "logicalLocations": [
      {
        "fullyQualifiedName": "dockerfile"
      }
    ]
  }
],
"Suppressions": [
  {
    "kind": "external"
  }
]
```

```
    ],
    "baselineState": "unchanged"
  },
  {
    "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2016-2781_deb_coreutils_8.32-4+b1",
    "ruleIndex": 0,
    "level": "warning",
    "message": {
      "text": "The path /var/lib/dpkg/status reports coreutils at version 8.32-4+b1 which is a
vulnerable (deb) package installed in the container",
      "id": "default"
    },
    "analysisTarget": {
      "uri": "/var/lib/dpkg/status"
    },
    "locations": [
      {
        "physicalLocation": {
          "artifactLocation": {
            "uri": "/var/lib/dpkg/status"
          },
          "region": {
            "startLine": 1,
            "startColumn": 1,
            "endLine": 1,
            "endColumn": 1,
            "byteOffset": 1,
            "byteLength": 1
          }
        }
      }
    ]
  }
}
```

```
    },
    "logicalLocations": [
      {
        "fullyQualifiedName": "dockerfile"
      }
    ]
  }
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2016-2781_deb_coreutils_8.32-4+b1",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports coreutils at version 8.32-4+b1 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
```



```
"physicalLocation": {
  "artifactLocation": {
    "uri": "/var/lib/dpkg/status"
  },
  "region": {
    "startLine": 1,
    "startColumn": 1,
    "endLine": 1,
    "endColumn": 1,
    "byteOffset": 1,
    "byteLength": 1
  }
},
"logicalLocations": [
  {
    "fullyQualifiedName": "dockerfile"
  }
]
},
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2017-11164_deb_libpcre3_2:8.39-13",
```

```
"ruleIndex": 0,
"level": "warning",
"message": {
  "text": "The path /var/lib/dpkg/status reports libpcre3 at version 2:8.39-13 which is a vulnerable
(deb) package installed in the container",
  "id": "default"
},
"analysisTarget": {
  "uri": "/var/lib/dpkg/status"
},
"locations": [
  {
    "physicalLocation": {
      "artifactLocation": {
        "uri": "/var/lib/dpkg/status"
      },
      "region": {
        "startLine": 1,
        "startColumn": 1,
        "endLine": 1,
        "endColumn": 1,
        "byteOffset": 1,
        "byteLength": 1
      }
    },
    "logicalLocations": [
      {
        "fullyQualifiedName": "dockerfile"
      }
    ]
  }
]
```

```
    ]
  }
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2017-16231_deb_libpcre3_2:8.39-13",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libpcre3 at version 2:8.39-13 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        }
      },
      "region": {
```

```
    "startLine": 1,
    "startColumn": 1,
    "endLine": 1,
    "endColumn": 1,
    "byteOffset": 1,
    "byteLength": 1
  }
},
"logicalLocations": [
  {
    "fullyQualifiedName": "dockerfile"
  }
]
},
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2017-18018_deb_coreutils_8.32-4+b1",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
```

"text": "The path /var/lib/dpkg/status reports coreutils at version 8.32-4+b1 which is a vulnerable (deb) package installed in the container",

"id": "default"

},

"analysisTarget": {

"uri": "/var/lib/dpkg/status"

},

"locations": [

{

"physicalLocation": {

"artifactLocation": {

"uri": "/var/lib/dpkg/status"

},

"region": {

"startLine": 1,

"startColumn": 1,

"endLine": 1,

"endColumn": 1,

"byteOffset": 1,

"byteLength": 1

}

},

"logicalLocations": [

{

"fullyQualifiedName": "dockerfile"

}

]

}

],

```
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2017-18018_deb_coreutils_8.32-4+b1",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports coreutils at version 8.32-4+b1 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        },
        "region": {
          "startLine": 1,
          "startColumn": 1,
```

```
    "endLine": 1,
    "endColumn": 1,
    "byteOffset": 1,
    "byteLength": 1
  }
},
"logicalLocations": [
  {
    "fullyQualifiedName": "dockerfile"
  }
]
},
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2017-7245_deb_libpcre3_2:8.39-13",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libpcre3 at version 2:8.39-13 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  }
},
```

```
"analysisTarget": {
  "uri": "/var/lib/dpkg/status"
},
"locations": [
  {
    "physicalLocation": {
      "artifactLocation": {
        "uri": "/var/lib/dpkg/status"
      },
      "region": {
        "startLine": 1,
        "startColumn": 1,
        "endLine": 1,
        "endColumn": 1,
        "byteOffset": 1,
        "byteLength": 1
      }
    },
    "logicalLocations": [
      {
        "fullyQualifiedName": "dockerfile"
      }
    ]
  }
],
"suppressions": [
  {
    "kind": "external"
  }
]
```



```
    ],  
    "baselineState": "unchanged"  
  },  
  {  
    "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2017-7246_deb_libpcre3_2:8.39-13",  
    "ruleIndex": 0,  
    "level": "warning",  
    "message": {  
      "text": "The path /var/lib/dpkg/status reports libpcre3 at version 2:8.39-13 which is a vulnerable  
(deb) package installed in the container",  
      "id": "default"  
    },  
    "analysisTarget": {  
      "uri": "/var/lib/dpkg/status"  
    },  
    "locations": [  
      {  
        "physicalLocation": {  
          "artifactLocation": {  
            "uri": "/var/lib/dpkg/status"  
          },  
          "region": {  
            "startLine": 1,  
            "startColumn": 1,  
            "endLine": 1,  
            "endColumn": 1,  
            "byteOffset": 1,  
            "byteLength": 1  
          }  
        }  
      ]  
    }  
  }  
}
```

```
    },
    "logicalLocations": [
      {
        "fullyQualifiedName": "dockerfile"
      }
    ]
  }
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2018-20796_deb_libc-bin_2.31-13",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libc-bin at version 2.31-13 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
```

```
"physicalLocation": {
  "artifactLocation": {
    "uri": "/var/lib/dpkg/status"
  },
  "region": {
    "startLine": 1,
    "startColumn": 1,
    "endLine": 1,
    "endColumn": 1,
    "byteOffset": 1,
    "byteLength": 1
  }
},
"logicalLocations": [
  {
    "fullyQualifiedName": "dockerfile"
  }
]
},
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2018-20796_deb_libc6_2.31-13",
```

```
"ruleIndex": 0,

"level": "warning",

"message": {

  "text": "The path /var/lib/dpkg/status reports libc6 at version 2.31-13 which is a vulnerable (deb)
package installed in the container",

  "id": "default"

},

"analysisTarget": {

  "uri": "/var/lib/dpkg/status"

},

"locations": [

{

  "physicalLocation": {

    "artifactLocation": {

      "uri": "/var/lib/dpkg/status"

    },

    "region": {

      "startLine": 1,

      "startColumn": 1,

      "endLine": 1,

      "endColumn": 1,

      "byteOffset": 1,

      "byteLength": 1

    }

  },

  "logicalLocations": [

    {

      "fullyQualifiedName": "dockerfile"

    }

  ]

}
```

```
    ]
  }
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2018-5709_deb_libgssapi-krb5-2_1.18.3-6",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libgssapi-krb5-2 at version 1.18.3-6 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        }
      },
    },
  ],
}
```

```
"region": {
  "startLine": 1,
  "startColumn": 1,
  "endLine": 1,
  "endColumn": 1,
  "byteOffset": 1,
  "byteLength": 1
},
"logicalLocations": [
  {
    "fullyQualifiedName": "dockerfile"
  }
]
},
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2018-5709_deb_libk5crypto3_1.18.3-6",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
```

"text": "The path /var/lib/dpkg/status reports libk5crypto3 at version 1.18.3-6 which is a vulnerable (deb) package installed in the container",

"id": "default"

},

"analysisTarget": {

"uri": "/var/lib/dpkg/status"

},

"locations": [

{

"physicalLocation": {

"artifactLocation": {

"uri": "/var/lib/dpkg/status"

},

"region": {

"startLine": 1,

"startColumn": 1,

"endLine": 1,

"endColumn": 1,

"byteOffset": 1,

"byteLength": 1

}

},

"logicalLocations": [

{

"fullyQualifiedName": "dockerfile"

}

]

}

],

```
"suppressions": [  
  {  
    "kind": "external"  
  }  
],  
"baselineState": "unchanged"  
},  
{  
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2018-5709_deb_libkrb5-3_1.18.3-6",  
  "ruleIndex": 0,  
  "level": "warning",  
  "message": {  
    "text": "The path /var/lib/dpkg/status reports libkrb5-3 at version 1.18.3-6 which is a vulnerable  
(deb) package installed in the container",  
    "id": "default"  
  },  
  "analysisTarget": {  
    "uri": "/var/lib/dpkg/status"  
  },  
  "locations": [  
    {  
      "physicalLocation": {  
        "artifactLocation": {  
          "uri": "/var/lib/dpkg/status"  
        },  
        "region": {  
          "startLine": 1,  
          "startColumn": 1,  
          "endLine": 1,  
          "endColumn": 1
```



```
        "endColumn": 1,
        "byteOffset": 1,
        "byteLength": 1
    }
},
"logicalLocations": [
    {
        "fullyQualifiedName": "dockerfile"
    }
]
},
"suppressions": [
    {
        "kind": "external"
    }
],
"baselineState": "unchanged"
},
{
    "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2018-5709_deb_libkrb5support0_1.18.3-6",
    "ruleIndex": 0,
    "level": "warning",
    "message": {
        "text": "The path /var/lib/dpkg/status reports libkrb5support0 at version 1.18.3-6 which is a vulnerable (deb) package installed in the container",
        "id": "default"
    }
},
```

```
"analysisTarget": {
  "uri": "/var/lib/dpkg/status"
},
"locations": [
  {
    "physicalLocation": {
      "artifactLocation": {
        "uri": "/var/lib/dpkg/status"
      },
      "region": {
        "startLine": 1,
        "startColumn": 1,
        "endLine": 1,
        "endColumn": 1,
        "byteOffset": 1,
        "byteLength": 1
      }
    },
    "logicalLocations": [
      {
        "fullyQualifiedName": "dockerfile"
      }
    ]
  }
],
"Suppressions": [
  {
    "kind": "external"
  }
]
```

```
    ],  
    "baselineState": "unchanged"  
  },  
  {  
    "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2018-6829_deb_libcrypt20_1.8.7-6",  
    "ruleIndex": 0,  
    "level": "warning",  
    "message": {  
      "text": "The path /var/lib/dpkg/status reports libcrypt20 at version 1.8.7-6 which is a vulnerable  
(deb) package installed in the container",  
      "id": "default"  
    },  
    "analysisTarget": {  
      "uri": "/var/lib/dpkg/status"  
    },  
    "locations": [  
      {  
        "physicalLocation": {  
          "artifactLocation": {  
            "uri": "/var/lib/dpkg/status"  
          },  
          "region": {  
            "startLine": 1,  
            "startColumn": 1,  
            "endLine": 1,  
            "endColumn": 1,  
            "byteOffset": 1,  
            "byteLength": 1  
          }  
        }  
      ]  
    }  
  }  
}
```

```
    },
    "logicalLocations": [
      {
        "fullyQualifiedName": "dockerfile"
      }
    ]
  }
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-1010022_deb_libc-bin_2.31-13",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libc-bin at version 2.31-13 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
```

```
"physicalLocation": {
  "artifactLocation": {
    "uri": "/var/lib/dpkg/status"
  },
  "region": {
    "startLine": 1,
    "startColumn": 1,
    "endLine": 1,
    "endColumn": 1,
    "byteOffset": 1,
    "byteLength": 1
  }
},
"logicalLocations": [
  {
    "fullyQualifiedName": "dockerfile"
  }
]
},
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-1010022_deb_libc6_2.31-13",
```

```
"ruleIndex": 0,

"level": "warning",

"message": {

  "text": "The path /var/lib/dpkg/status reports libc6 at version 2.31-13 which is a vulnerable (deb)
package installed in the container",

  "id": "default"

},

"analysisTarget": {

  "uri": "/var/lib/dpkg/status"

},

"locations": [

{

  "physicalLocation": {

    "artifactLocation": {

      "uri": "/var/lib/dpkg/status"

    },

    "region": {

      "startLine": 1,

      "startColumn": 1,

      "endLine": 1,

      "endColumn": 1,

      "byteOffset": 1,

      "byteLength": 1

    }

  },

  "logicalLocations": [

    {

      "fullyQualifiedName": "dockerfile"

    }

  ]

}
```

```
    ]
  }
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-1010023_deb_libc-bin_2.31-13",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libc-bin at version 2.31-13 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        }
      },
      "region": {
```

```
    "startLine": 1,
    "startColumn": 1,
    "endLine": 1,
    "endColumn": 1,
    "byteOffset": 1,
    "byteLength": 1
  }
},
"logicalLocations": [
  {
    "fullyQualifiedName": "dockerfile"
  }
]
}
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-1010023_deb_libc6_2.31-13",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libc6 at version 2.31-13 which is a vulnerable (deb) package installed in the container",
```



```
"id": "default"
},
"analysisTarget": {
  "uri": "/var/lib/dpkg/status"
},
"locations": [
  {
    "physicalLocation": {
      "artifactLocation": {
        "uri": "/var/lib/dpkg/status"
      },
      "region": {
        "startLine": 1,
        "startColumn": 1,
        "endLine": 1,
        "endColumn": 1,
        "byteOffset": 1,
        "byteLength": 1
      }
    },
    "logicalLocations": [
      {
        "fullyQualifiedName": "dockerfile"
      }
    ]
  }
],
"suppressions": [
  {
```

```
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-1010024_deb_libc-bin_2.31-13",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libc-bin at version 2.31-13 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        },
        "region": {
          "startLine": 1,
          "startColumn": 1,
          "endLine": 1,
          "endColumn": 1,
          "byteOffset": 1,

```

```
      "byteLength": 1
    },
    "logicalLocations": [
      {
        "fullyQualifiedName": "dockerfile"
      }
    ]
  },
  "suppressions": [
    {
      "kind": "external"
    }
  ],
  "baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-1010024_deb_libc6_2.31-13",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libc6 at version 2.31-13 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  }
},
```

```
"locations": [  
  {  
    "physicalLocation": {  
      "artifactLocation": {  
        "uri": "/var/lib/dpkg/status"  
      },  
      "region": {  
        "startLine": 1,  
        "startColumn": 1,  
        "endLine": 1,  
        "endColumn": 1,  
        "byteOffset": 1,  
        "byteLength": 1  
      }  
    },  
    "logicalLocations": [  
      {  
        "fullyQualifiedName": "dockerfile"  
      }  
    ]  
  },  
  {  
    "suppressions": [  
      {  
        "kind": "external"  
      }  
    ],  
    "baselineState": "unchanged"  
  },  
]
```

```
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-1010025_deb_libc-bin_2.31-13",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libc-bin at version 2.31-13 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        },
        "region": {
          "startLine": 1,
          "startColumn": 1,
          "endLine": 1,
          "endColumn": 1,
          "byteOffset": 1,
          "byteLength": 1
        }
      },
      "logicalLocations": [
        {
```

```
        "fullyQualifiedName": "dockerfile"
      }
    ]
  },
  ],
  "suppressions": [
    {
      "kind": "external"
    }
  ],
  "baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-1010025_deb_libc6_2.31-13",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libc6 at version 2.31-13 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        }
      }
    }
  ]
}
```

```
    },
    "region": {
      "startLine": 1,
      "startColumn": 1,
      "endLine": 1,
      "endColumn": 1,
      "byteOffset": 1,
      "byteLength": 1
    }
  },
  "logicalLocations": [
    {
      "fullyQualifiedName": "dockerfile"
    }
  ]
},
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-19882_deb_login_1:4.8.1-1",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
```

"text": "The path /var/lib/dpkg/status reports login at version 1:4.8.1-1 which is a vulnerable (deb) package installed in the container",

"id": "default"

},

"analysisTarget": {

"uri": "/var/lib/dpkg/status"

},

"locations": [

{

"physicalLocation": {

"artifactLocation": {

"uri": "/var/lib/dpkg/status"

},

"region": {

"startLine": 1,

"startColumn": 1,

"endLine": 1,

"endColumn": 1,

"byteOffset": 1,

"byteLength": 1

}

},

"logicalLocations": [

{

"fullyQualifiedName": "dockerfile"

}

]

}

],


```
"suppressions": [  
  {  
    "kind": "external"  
  }  
],  
"baselineState": "unchanged"  
},  
{  
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-19882_deb_passwd_1:4.8.1-1",  
  "ruleIndex": 0,  
  "level": "warning",  
  "message": {  
    "text": "The path /var/lib/dpkg/status reports passwd at version 1:4.8.1-1 which is a vulnerable  
(deb) package installed in the container",  
    "id": "default"  
  },  
  "analysisTarget": {  
    "uri": "/var/lib/dpkg/status"  
  },  
  "locations": [  
    {  
      "physicalLocation": {  
        "artifactLocation": {  
          "uri": "/var/lib/dpkg/status"  
        },  
        "region": {  
          "startLine": 1,  
          "startColumn": 1,  
          "endLine": 1,
```

```
        "endColumn": 1,
        "byteOffset": 1,
        "byteLength": 1
    }
},
"logicalLocations": [
    {
        "fullyQualifiedName": "dockerfile"
    }
]
},
"suppressions": [
    {
        "kind": "external"
    }
],
"baselineState": "unchanged"
},
{
    "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-20838_deb_libpcre3_2:8.39-13",
    "ruleIndex": 0,
    "level": "warning",
    "message": {
        "text": "The path /var/lib/dpkg/status reports libpcre3 at version 2:8.39-13 which is a vulnerable (deb) package installed in the container",
        "id": "default"
    }
},
"analysisTarget": {
```

```
"uri": "/var/lib/dpkg/status"
},
"locations": [
  {
    "physicalLocation": {
      "artifactLocation": {
        "uri": "/var/lib/dpkg/status"
      },
      "region": {
        "startLine": 1,
        "startColumn": 1,
        "endLine": 1,
        "endColumn": 1,
        "byteOffset": 1,
        "byteLength": 1
      }
    },
    "logicalLocations": [
      {
        "fullyQualifiedName": "dockerfile"
      }
    ]
  }
],
"suppressions": [
  {
    "kind": "external"
  }
],
```

```
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-9192_deb_libc-bin_2.31-13",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libc-bin at version 2.31-13 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        },
        "region": {
          "startLine": 1,
          "startColumn": 1,
          "endLine": 1,
          "endColumn": 1,
          "byteOffset": 1,
          "byteLength": 1
        }
      }
    }
  ],
}
```

```
"logicalLocations": [  
  {  
    "fullyQualifiedName": "dockerfile"  
  }  
]  
}  
],  
"suppressions": [  
  {  
    "kind": "external"  
  }  
],  
"baselineState": "unchanged"  
},  
{  
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2019-9192_deb_libc6_2.31-13",  
  "ruleIndex": 0,  
  "level": "warning",  
  "message": {  
    "text": "The path /var/lib/dpkg/status reports libc6 at version 2.31-13 which is a vulnerable (deb)  
package installed in the container",  
    "id": "default"  
  },  
  "analysisTarget": {  
    "uri": "/var/lib/dpkg/status"  
  },  
  "locations": [  
    {  
      "physicalLocation": {
```

```

    "artifactLocation": {
      "uri": "/var/lib/dpkg/status"
    },
    "region": {
      "startLine": 1,
      "startColumn": 1,
      "endLine": 1,
      "endColumn": 1,
      "byteOffset": 1,
      "byteLength": 1
    }
  },
  "logicalLocations": [
    {
      "fullyQualifiedName": "dockerfile"
    }
  ]
},
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2020-13529_deb_libsystemd0_247.3-6",

```

```
"ruleIndex": 0,

"level": "warning",

"message": {

  "text": "The path /var/lib/dpkg/status reports libsystemd0 at version 247.3-6 which is a
vulnerable (deb) package installed in the container",

  "id": "default"

},

"analysisTarget": {

  "uri": "/var/lib/dpkg/status"

},

"locations": [

{

  "physicalLocation": {

    "artifactLocation": {

      "uri": "/var/lib/dpkg/status"

    },

    "region": {

      "startLine": 1,

      "startColumn": 1,

      "endLine": 1,

      "endColumn": 1,

      "byteOffset": 1,

      "byteLength": 1

    }

  },

  "logicalLocations": [

    {

      "fullyQualifiedName": "dockerfile"

    }

  ]

}
```

```
    ]
  }
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2020-13529_deb_libudev1_247.3-6",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libudev1 at version 247.3-6 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        }
      },
      "region": {
```



```
    "startLine": 1,
    "startColumn": 1,
    "endLine": 1,
    "endColumn": 1,
    "byteOffset": 1,
    "byteLength": 1
  }
},
"logicalLocations": [
  {
    "fullyQualifiedName": "dockerfile"
  }
]
}
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-33574_deb_libc-bin_2.31-13",
  "ruleIndex": 0,
  "level": "error",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libc-bin at version 2.31-13 which is a vulnerable (deb) package installed in the container",
```

```
"id": "default"
},
"analysisTarget": {
  "uri": "/var/lib/dpkg/status"
},
"locations": [
  {
    "physicalLocation": {
      "artifactLocation": {
        "uri": "/var/lib/dpkg/status"
      },
      "region": {
        "startLine": 1,
        "startColumn": 1,
        "endLine": 1,
        "endColumn": 1,
        "byteOffset": 1,
        "byteLength": 1
      }
    },
    "logicalLocations": [
      {
        "fullyQualifiedName": "dockerfile"
      }
    ]
  }
],
"suppressions": [
  {
```

```
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-33574_deb_libc6_2.31-13",
  "ruleIndex": 0,
  "level": "error",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libc6 at version 2.31-13 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        },
        "region": {
          "startLine": 1,
          "startColumn": 1,
          "endLine": 1,
          "endColumn": 1,
          "byteOffset": 1,

```

```
        "byteLength": 1
      }
    },
    "logicalLocations": [
      {
        "fullyQualifiedName": "dockerfile"
      }
    ]
  }
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-36084_deb_libsepol1_3.1-1",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libsepol1 at version 3.1-1 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  }
},
```

```
"locations": [  
  {  
    "physicalLocation": {  
      "artifactLocation": {  
        "uri": "/var/lib/dpkg/status"  
      },  
      "region": {  
        "startLine": 1,  
        "startColumn": 1,  
        "endLine": 1,  
        "endColumn": 1,  
        "byteOffset": 1,  
        "byteLength": 1  
      }  
    },  
    "logicalLocations": [  
      {  
        "fullyQualifiedName": "dockerfile"  
      }  
    ]  
  },  
  {  
    "suppressions": [  
      {  
        "kind": "external"  
      }  
    ],  
    "baselineState": "unchanged"  
  },  
]
```

```
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-36085_deb_libsepol1_3.1-1",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libsepol1 at version 3.1-1 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        },
        "region": {
          "startLine": 1,
          "startColumn": 1,
          "endLine": 1,
          "endColumn": 1,
          "byteOffset": 1,
          "byteLength": 1
        }
      },
      "logicalLocations": [
        {
```

```
        "fullyQualifiedName": "dockerfile"
      }
    ]
  },
  ],
  "suppressions": [
    {
      "kind": "external"
    }
  ],
  "baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-36086_deb_libsepol1_3.1-1",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libsepol1 at version 3.1-1 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        }
      }
    }
  ]
}
```

```
    },
    "region": {
      "startLine": 1,
      "startColumn": 1,
      "endLine": 1,
      "endColumn": 1,
      "byteOffset": 1,
      "byteLength": 1
    }
  },
  "logicalLocations": [
    {
      "fullyQualifiedName": "dockerfile"
    }
  ]
},
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-36087_deb_libsepol1_3.1-1",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
```


"text": "The path /var/lib/dpkg/status reports libsepol1 at version 3.1-1 which is a vulnerable (deb) package installed in the container",

"id": "default"

},

"analysisTarget": {

"uri": "/var/lib/dpkg/status"

},

"locations": [

{

"physicalLocation": {

"artifactLocation": {

"uri": "/var/lib/dpkg/status"

},

"region": {

"startLine": 1,

"startColumn": 1,

"endLine": 1,

"endColumn": 1,

"byteOffset": 1,

"byteLength": 1

}

},

"logicalLocations": [

{

"fullyQualifiedName": "dockerfile"

}

]

}

],

```
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-36690_deb_libsqlite3-0_3.34.1-3",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libsqlite3-0 at version 3.34.1-3 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        },
        "region": {
          "startLine": 1,
          "startColumn": 1,
```

```
    "endLine": 1,
    "endColumn": 1,
    "byteOffset": 1,
    "byteLength": 1
  }
},
"logicalLocations": [
  {
    "fullyQualifiedName": "dockerfile"
  }
]
},
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-37750_deb_libgssapi-krb5-2_1.18.3-6",
  "ruleIndex": 0,
  "level": "error",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libgssapi-krb5-2 at version 1.18.3-6 which is a vulnerable (deb) package installed in the container",
    "id": "default"
```

```
},
"analysisTarget": {
  "uri": "/var/lib/dpkg/status"
},
"locations": [
  {
    "physicalLocation": {
      "artifactLocation": {
        "uri": "/var/lib/dpkg/status"
      },
      "region": {
        "startLine": 1,
        "startColumn": 1,
        "endLine": 1,
        "endColumn": 1,
        "byteOffset": 1,
        "byteLength": 1
      }
    },
    "logicalLocations": [
      {
        "fullyQualifiedName": "dockerfile"
      }
    ]
  }
],
"Suppressions": [
  {
    "kind": "external"
```

```
    }
  ],
  "baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-37750_deb_libk5crypto3_1.18.3-6",
  "ruleIndex": 0,
  "level": "error",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libk5crypto3 at version 1.18.3-6 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        }
      },
      "region": {
        "startLine": 1,
        "startColumn": 1,
        "endLine": 1,
        "endColumn": 1,
        "byteOffset": 1,

```

```
        "byteLength": 1
      }
    },
    "logicalLocations": [
      {
        "fullyQualifiedName": "dockerfile"
      }
    ]
  }
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-37750_deb_libkrb5-3_1.18.3-6",
  "ruleIndex": 0,
  "level": "error",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libkrb5-3 at version 1.18.3-6 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  }
},
```

```
"locations": [  
  {  
    "physicalLocation": {  
      "artifactLocation": {  
        "uri": "/var/lib/dpkg/status"  
      },  
      "region": {  
        "startLine": 1,  
        "startColumn": 1,  
        "endLine": 1,  
        "endColumn": 1,  
        "byteOffset": 1,  
        "byteLength": 1  
      }  
    },  
    "logicalLocations": [  
      {  
        "fullyQualifiedName": "dockerfile"  
      }  
    ]  
  },  
  {  
    "suppressions": [  
      {  
        "kind": "external"  
      }  
    ],  
    "baselineState": "unchanged"  
  },  
]
```

```
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-37750_deb_libkrb5support0_1.18.3-6",
  "ruleIndex": 0,
  "level": "error",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libkrb5support0 at version 1.18.3-6 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        },
        "region": {
          "startLine": 1,
          "startColumn": 1,
          "endLine": 1,
          "endColumn": 1,
          "byteOffset": 1,
          "byteLength": 1
        }
      },
      "logicalLocations": [
```



```
{
  "fullyQualifiedName": "dockerfile"
}
]
}
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-39537_deb_libncursesw6_6.2+20201114-2",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libncursesw6 at version 6.2+20201114-2 which is a vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
```

```
"artifactLocation": {
  "uri": "/var/lib/dpkg/status"
},
"region": {
  "startLine": 1,
  "startColumn": 1,
  "endLine": 1,
  "endColumn": 1,
  "byteOffset": 1,
  "byteLength": 1
}
},
"logicalLocations": [
  {
    "fullyQualifiedName": "dockerfile"
  }
]
},
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-39537_deb_libtinfo6_6.2+20201114-2",
```

```
"ruleIndex": 0,

"level": "warning",

"message": {

  "text": "The path /var/lib/dpkg/status reports libtinfo6 at version 6.2+20201114-2 which is a
vulnerable (deb) package installed in the container",

  "id": "default"

},

"analysisTarget": {

  "uri": "/var/lib/dpkg/status"

},

"locations": [

{

  "physicalLocation": {

    "artifactLocation": {

      "uri": "/var/lib/dpkg/status"

    },

    "region": {

      "startLine": 1,

      "startColumn": 1,

      "endLine": 1,

      "endColumn": 1,

      "byteOffset": 1,

      "byteLength": 1

    }

  },

  "logicalLocations": [

    {

      "fullyQualifiedName": "dockerfile"

    }

  ]

}
```

```
    ]
  }
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-39537_deb_ncurses-
base_6.2+20201114-2",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
    "text": "The path /var/lib/dpkg/status reports ncurses-base at version 6.2+20201114-2 which is a
vulnerable (deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        }
      },
    },
  ],
}
```

```
"region": {
  "startLine": 1,
  "startColumn": 1,
  "endLine": 1,
  "endColumn": 1,
  "byteOffset": 1,
  "byteLength": 1
},
"logicalLocations": [
  {
    "fullyQualifiedName": "dockerfile"
  }
],
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-39537_deb_ncurses-
bin_6.2+20201114-2",
  "ruleIndex": 0,
  "level": "warning",
  "message": {
```

"text": "The path /var/lib/dpkg/status reports ncurses-bin at version 6.2+20201114-2 which is a vulnerable (deb) package installed in the container",

"id": "default"

},

"analysisTarget": {

"uri": "/var/lib/dpkg/status"

},

"locations": [

{

"physicalLocation": {

"artifactLocation": {

"uri": "/var/lib/dpkg/status"

},

"region": {

"startLine": 1,

"startColumn": 1,

"endLine": 1,

"endColumn": 1,

"byteOffset": 1,

"byteLength": 1

}

},

"logicalLocations": [

{

"fullyQualifiedName": "dockerfile"

}

]

}

],

```
"suppressions": [
  {
    "kind": "external"
  }
],
"baselineState": "unchanged"
},
{
  "ruleId": "ANCHOREVULN_localbuild/testimage:latest_CVE-2021-40528_deb_libgrypt20_1.8.7-6",
  "ruleIndex": 0,
  "level": "error",
  "message": {
    "text": "The path /var/lib/dpkg/status reports libgrypt20 at version 1.8.7-6 which is a vulnerable
(deb) package installed in the container",
    "id": "default"
  },
  "analysisTarget": {
    "uri": "/var/lib/dpkg/status"
  },
  "locations": [
    {
      "physicalLocation": {
        "artifactLocation": {
          "uri": "/var/lib/dpkg/status"
        },
        "region": {
          "startLine": 1,
          "startColumn": 1,
          "endLine": 1,
```

```
        "endColumn": 1,
        "byteOffset": 1,
        "byteLength": 1
    }
},
"logicalLocations": [
    {
        "fullyQualifiedName": "dockerfile"
    }
]
},
"suppressions": [
    {
        "kind": "external"
    }
],
"baselineState": "unchanged"
}
],
"columnKind": "utf16CodeUnits"
}
]
}
```