GCVE-1-2025-0002 - Vulnerability-Lookup

Archived: 2026-04-05 21:47:13 UTC


```
{
   "containers": {
      "cna": {
         "affected": [
            {
               "defaultStatus": "unaffected",
               "product": "exfiltration",
               "vendor": "Cl0p ransomware",
               "versions": [
                  {
                     "status": "affected",
                  },
               ],
            },
         ],
         "credits": [
            {
               "lang": "en",
               "type": "finder",
               "value": "Lorenzo Nicolodi",
            },
         ],
         "descriptions": [
            {
               "lang": "en",
               "supportingMedia": [
                  {
                     "base64": false,
                     "type": "text/html",
                     "value": "<div>The Python-based data-exfiltration utility used by the Cl0p ransc
                  },
               ],
               "value": "The Python-based data-exfiltration utility used by the Cl0p ransomware group
            },
         ],
         "impacts": [
            {
               "capecId": "CAPEC-549",
               "descriptions": [
                  {
```

```
                "lang": "en",
                "value": "CAPEC-549 Local Execution of Code",
             },
          ],
       },
    ],
    "metrics": [
       {
          "cvssV4_0": {
             "Automatable": "YES",
             "Recovery": "NOT_DEFINED",
             "Safety": "NOT_DEFINED",
             "attackComplexity": "LOW",
             "attackRequirements": "PRESENT",
             "attackVector": "NETWORK",
             "baseScore": 8.9,
             "baseSeverity": "HIGH",
             "privilegesRequired": "NONE",
             "providerUrgency": "NOT_DEFINED",
             "subAvailabilityImpact": "HIGH",
             "subConfidentialityImpact": "HIGH",
             "subIntegrityImpact": "HIGH",
             "userInteraction": "ACTIVE",
             "valueDensity": "NOT_DEFINED",
             "vectorString": "CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:A/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/A
             "version": "4.0",
             "vulnAvailabilityImpact": "HIGH",
             "vulnConfidentialityImpact": "HIGH",
             "vulnIntegrityImpact": "HIGH",
             "vulnerabilityResponseEffort": "NOT_DEFINED",
          },
          "format": "CVSS",
          "scenarios": [
             {
                "lang": "en",
                "value": "GENERAL",
             },
          ],
       },
    ],
    "problemTypes": [
       {
          "descriptions": [
             {
                "cweId": "CWE-20",
                "description": "CWE-20 Improper Input Validation",
                "lang": "en",
```

```
                  "type": "CWE",
               },
            ],
         },
      ],
      "providerMetadata": {
         "orgId": "00000000-0000-4000-9000-000000000000",
      },
      "references": [
         {
            "tags": [
               "related",
            ],
            "url": "https://amnwxasjtjc6e42siac6t45mhbkgtycrx5krv7sf5festvqxmnchuayd.onion",
         },
         {
            "tags": [
               "related",
            ],
            "url": "https://www.hackthebox.com/blog/cve-2023-34362-explained",
         },
      ],
      "source": {
         "discovery": "UNKNOWN",
      },
      "title": "Command Injection in Cl0p Exfiltration Python Script",
      "x_generator": {
         "engine": "Vulnogram 0.2.0",
      },
   },
},
"cveMetadata": {
   "assignerOrgId": "00000000-0000-4000-9000-000000000000",
   "datePublished": "2025-07-01T08:19:00.000Z",
   "dateUpdated": "2025-07-01T10:58:58.443468Z",
   "requesterUserId": "00000000-0000-4000-9000-000000000000",
   "serial": 1,
   "state": "PUBLISHED",
   "vulnId": "GCVE-1-2025-0002",
   "vulnerabilitylookup_history": [
      [
         "alexandre.dulaunoy@circl.lu",
         "2025-07-01T08:19:55.399348Z",
      ],
      [
         "alexandre.dulaunoy@circl.lu",
         "2025-07-01T08:23:59.977382Z",
```

```
         ],
         [
            "alexandre.dulaunoy@circl.lu",
            "2025-07-01T10:58:58.443468Z",
         ],
      ],
   },
   "dataType": "CVE_RECORD",
   "dataVersion": "5.1",
}
```
