**EXTRACT WHAT IS IN RED**

**SEPARATE FIELDS USING “|”**

Example, Record 1, separated by newline:

"CVE-2023-0001" | “psirt@paloaltonetworks.com" | "CWE-319" "https://security.paloaltonetworks.com/CVE-2023-0001", "https://security.paloaltonetworks.com/CVE-2023-0002" | "An information exposure vulnerability in the Palo Alto Networks Cortex XDR agent on Windows devices allows a local system administrator to disclose the admin password for the agent in cleartext, which bad actors can then use to execute privileged cytool commands that disable or uninstall the agent." | cpe:2.3:a:paloaltonetworks:cortex\_xdr\_agent:\*:\*:\*:\*:critical\_environment:\*:\*:\*", "7.5", "7.5.101" | "LOCAL" | "LOW" | "HIGH" | "NONE" | "HIGH" | "HIGH" | "HIGH" | "MEDIUM"**\n**

Example Record to Process:

"CVE\_data\_meta" : {

"ID" : "CVE-2023-0001",

"ASSIGNER" : "psirt@paloaltonetworks.com"

},

"problemtype" : {

"problemtype\_data" : [ {

"description" : [ {

"lang" : "en",

"value" : "CWE-319"

} ]

} ]

},

"references" : {

"reference\_data" : [ {

"url" : "https://security.paloaltonetworks.com/CVE-2023-0001",

"name" : "https://security.paloaltonetworks.com/CVE-2023-0001",

"refsource" : "MISC",

"tags" : [ "Vendor Advisory" ]

} ]

},

"description" : {

"description\_data" : [ {

"lang" : "en",

"value" : "An information exposure vulnerability in the Palo Alto Networks Cortex XDR agent on Windows devices allows a local system administrator to disclose the admin password for the agent in cleartext, which bad actors can then use to execute privileged cytool commands that disable or uninstall the agent."

} ]

}

},

"configurations" : {

"CVE\_data\_version" : "4.0",

"nodes" : [ {

"operator" : "AND",

"children" : [ {

"operator" : "OR",

"children" : [ ],

"cpe\_match" : [ {

"vulnerable" : true,

"cpe23Uri" : "cpe:2.3:a:paloaltonetworks:cortex\_xdr\_agent:\*:\*:\*:\*:critical\_environment:\*:\*:\*",

"versionStartIncluding" : "7.5",

"versionEndExcluding" : "7.5.101",

"cpe\_name" : [ ]

} ]

}, {

"operator" : "OR",

"children" : [ ],

"cpe\_match" : [ {

"vulnerable" : false,

"cpe23Uri" : "cpe:2.3:o:microsoft:windows:-:\*:\*:\*:\*:\*:\*:\*",

"cpe\_name" : [ ]

} ]

} ],

"cpe\_match" : [ ]

} ]

},

"impact" : {

"baseMetricV3" : {

"cvssV3" : {

"version" : "3.1",

"vectorString" : "CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H",

"attackVector" : "LOCAL",

"attackComplexity" : "LOW",

"privilegesRequired" : "HIGH",

"userInteraction" : "NONE",

"scope" : "UNCHANGED",

"confidentialityImpact" : "HIGH",

"integrityImpact" : "HIGH",

"availabilityImpact" : "HIGH",

"baseScore" : 6.7,

"baseSeverity" : "MEDIUM"

},

"exploitabilityScore" : 0.8,

"impactScore" : 5.9

}

},

"publishedDate" : "2023-02-08T18:15Z",

"lastModifiedDate" : "2023-02-18T20:41Z"

}