**FILE FORMAT**

{

"CVE\_data\_type" : "CVE",

"CVE\_data\_format" : "MITRE",

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

"CVE\_data\_numberOfCVEs" : "11745",

"CVE\_data\_timestamp" : "2023-07-27T07:00Z",

"CVE\_Items" : [ {

"cve" : {

"data\_type" : "CVE",

"data\_format" : "MITRE",

"data\_version" : "4.0",

"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"

}, {

"cve" : {

"data\_type" : "CVE",

"data\_format" : "MITRE",

"data\_version" : "4.0",

"CVE\_data\_meta" : {

"ID" : "CVE-2023-0002",

"ASSIGNER" : "psirt@paloaltonetworks.com"

},

"problemtype" : {

"problemtype\_data" : [ {

"description" : [ {

"lang" : "en",

"value" : "NVD-CWE-Other"

} ]

} ]

},

"references" : {

"reference\_data" : [ {

"url" : "https://security.paloaltonetworks.com/CVE-2023-0002",

"name" : "https://security.paloaltonetworks.com/CVE-2023-0002",

"refsource" : "MISC",

"tags" : [ "Vendor Advisory" ]

} ]

},

"description" : {

"description\_data" : [ {

"lang" : "en",

"value" : "A problem with a protection mechanism in the Palo Alto Networks Cortex XDR agent on Windows devices allows a local user 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:\*:\*:\*:\*:\*:\*:\*:\*",

"versionStartIncluding" : "5.0",

"versionEndExcluding" : "5.0.12.22203",

"cpe\_name" : [ ]

}, {

"vulnerable" : true,

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

"versionStartIncluding" : "7.5",

"versionEndIncluding" : "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:L/UI:N/S:U/C:H/I:H/A:H",

"attackVector" : "LOCAL",

"attackComplexity" : "LOW",

"privilegesRequired" : "LOW",

"userInteraction" : "NONE",

"scope" : "UNCHANGED",

"confidentialityImpact" : "HIGH",

"integrityImpact" : "HIGH",

"availabilityImpact" : "HIGH",

"baseScore" : 7.8,

"baseSeverity" : "HIGH"

},

"exploitabilityScore" : 1.8,

"impactScore" : 5.9

}

},

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

"lastModifiedDate" : "2023-02-18T20:45Z"

},

. . . . .

. . . . .

. . . . .

. . . . .

}, {

"cve" : {

"data\_type" : "CVE",

"data\_format" : "MITRE",

"data\_version" : "4.0",

"CVE\_data\_meta" : {

"ID" : "CVE-2023-3947",

"ASSIGNER" : "security@wordfence.com"

},

"problemtype" : {

"problemtype\_data" : [ {

"description" : [ {

"lang" : "en",

"value" : "CWE-321"

} ]

} ]

},

"references" : {

"reference\_data" : [ {

"url" : "https://plugins.trac.wordpress.org/browser/video-conferencing-with-zoom-api/trunk/includes/Helpers/Encryption.php?rev=2942302",

"name" : "https://plugins.trac.wordpress.org/browser/video-conferencing-with-zoom-api/trunk/includes/Helpers/Encryption.php?rev=2942302",

"refsource" : "MISC",

"tags" : [ ]

}, {

"url" : "https://www.wordfence.com/threat-intel/vulnerabilities/id/ba2515d9-ced0-4b49-87c4-04c8391c2608?source=cve",

"name" : "https://www.wordfence.com/threat-intel/vulnerabilities/id/ba2515d9-ced0-4b49-87c4-04c8391c2608?source=cve",

"refsource" : "MISC",

"tags" : [ ]

}, {

"url" : "https://plugins.trac.wordpress.org/browser/video-conferencing-with-zoom-api/tags/4.2.1/includes/helpers.php#L546",

"name" : "https://plugins.trac.wordpress.org/browser/video-conferencing-with-zoom-api/tags/4.2.1/includes/helpers.php#L546",

"refsource" : "MISC",

"tags" : [ ]

} ]

},

"description" : {

"description\_data" : [ {

"lang" : "en",

"value" : "The Video Conferencing with Zoom plugin for WordPress is vulnerable to Sensitive Information Exposure due to hardcoded encryption key on the 'vczapi\_encrypt\_decrypt' function in versions up to, and including, 4.2.1. This makes it possible for unauthenticated attackers to decrypt and view the meeting id and password."

} ]

}

},

"configurations" : {

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

"nodes" : [ ]

},

"impact" : {

"baseMetricV3" : {

"cvssV3" : {

"version" : "3.1",

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

"attackVector" : "NETWORK",

"attackComplexity" : "HIGH",

"privilegesRequired" : "NONE",

"userInteraction" : "NONE",

"scope" : "UNCHANGED",

"confidentialityImpact" : "LOW",

"integrityImpact" : "NONE",

"availabilityImpact" : "NONE",

"baseScore" : 3.7,

"baseSeverity" : "LOW"

},

"exploitabilityScore" : 2.2,

"impactScore" : 1.4

}

},

"publishedDate" : "2023-07-26T04:15Z",

"lastModifiedDate" : "2023-07-26T04:24Z"

} ]

}