CVE-2022-21828

Share

CVE-2015-4596
CVE-2015-5384
CVE-2015-5462
CVE-2015-5463
CVE-2015-5606
CVE-2016-1159
CVE-2016-1161
CVE-2017-1282
CVE-2017-1331
CVE-2018-10206
CVE-2018-10207
CVE-2018-10208
CVE-2018-10209
CVE-2018-10210
CVE-2018-10211
CVE-2018-10212
CVE-2018-10213
CVE-2018-15631
CVE-2018-18466
CVE-2018-20237
CVE-2018-20664
CVE-2018-20736
CVE-2018-20737
CVE-2019-11032
CVE-2019-12959
CVE-2019-12994
CVE-2019-14693
CVE-2019-16202
CVE-2019-1712
CVE-2019-19610
CVE-2019-19611
CVE-2019-19612
CVE-2019-19613
CVE-2019-19614
CVE-2019-20474
CVE-2019-3905
CVE-2019-6512
CVE-2019-6513
CVE-2019-6514
CVE-2019-6515
CVE-2019-6516
CVE-2019-6970
CVE-2019-7161
CVE-2019-7162
CVE-2019-9676
CVE-2020-15594
CVE-2020-15595
CVE-2020-20167
CVE-2020-26546
CVE-2020-28401
CVE-2020-28402
CVE-2020-28403
CVE-2020-28404
CVE-2020-28405
CVE-2020-28406
CVE-2020-28918
CVE-2020-8422
CVE-2021- 42110
CVE-2021- 44035
CVE-2021-31160
CVE-2021-31199
CVE-2021-31530
CVE-2021-31531
CVE-2021-31777
CVE-2021-32016
CVE-2021-32017
CVE-2021-32018
CVE-2021-38615
CVE-2021-38616
CVE-2021-38617
CVE-2021-38618
CVE-2021-41320
CVE-2021-42711
CVE-2021-43978
CVE-2022-0028
CVE-2022-21828
CVE-2022-22571
CVE-2022-22572
CVE-2022-24446
CVE-2022-24447
CVE-2022-24967
CVE-2022-29931
CVE-2022-30332
CVE-2022-34908
CVE-2022-34909
CVE-2022-34910
CVE-2022-36441
CVE-2022-36442
CVE-2022-36443
CVE-2022-37028
CVE-2022-38481
CVE-2022-38482
CVE-2022-41364
CVE-2022-41365
CVE-2022-41366
CVE-2022-41367
CVE-2023-26097
CVE-2023-26098
CVE-2023-26099
CVE-2023-27565
CVE-2023-28750
CVE-2023-28751
CVE-2023-28752
CVE-2023-29505
CVE-2023-31223
CVE-2023-35791
CVE-2023-35792
CVE-2023-41103
CVE-2023-48644
CVE-2023-48645
CVE-2023-50872
CVE-2023-51770
CVE-2023-51771
CVE-2024-24720
CVE-2024-24721
CVE-2024-25676
CVE-2024-28060
CVE-2024-28061
CVE-2024-38815
XLM-2016-121
XLM-2018-356
XLM-2019-672
XLM-2019-712
XLM-2020-1347
XLM-2024-6203
XLM-2024-6482
XLM-2024-6483
XLM-2024-6484

Abstract Advisory Information

A user with high privilege access to the Incappitic Connect web console can remotely execute code on the Incappitic Connect server using an unspecified attack vector in Incappitic Connect version 1.40.0, 1.39.1, 1.39.0, 1.38.1, 1.38.0, 1.37.1, 1.37.0, 1.36.0, 1.35.5, 1.35.4 and 1.35.3.

Authors: Dominique Righetto from Excellium Services

Version affected

Name: Incappitic
Versions: Incappitic Connect versions 1.40.0, 1.39.1, 1.39.0, 1.38.1, 1.38.0, 1.37.1, 1.37.0, 1.36.0, 1.35.5, 1.35.4 and 1.35.3.

Common Vulnerability Scoring System

9.1 – 3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Patches

version 1.40.1

References

- https://forums.ivanti.com/s/article/SA-2022-02-23?language=en_US
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-21828

Vulnerability Disclosure Timeline

- 18/02/2022: Vulnerability discovery
- 18/02/2022: Vulnerability Report to CERT XLM
- 21/02/2022: Vulnerability Report to Vendor
- 22/02/2022: Acknowledge from vendor
- 23/02/2022: CVE ID requested by vendor
- 23/02/2022: CVE ID assigned CVE-2022-21828
- 24/02/2022: Bug fixed and security advisory published
- 18/03/2022: Contacted vendor to update CVSS score
- 21/03/2022: Vendor answered they can't modify it.
- 04/04/2022: Security advisory published

Find more vulnerabilities in our Security Advisory section.