DJ-CERT | Centre national de veille, d'alerte et de réponse aux attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 05-11-2023

BULLETIN ALERTES

Object	Multiples vulnérabilités dans les produits Cisco
Réference	1064
Date de Publication	2023-11-03
Sévérité	Critique

IMPACT :

- Exécution du code arbitraire à distance
- Élévation de privilèges
- Contournement de la politique de sécurité
- Déni de service

SYSTÉME AFFECTÉ :

- Cisco Adaptive Security Appliance (ASA)
- Cisco Firepower Management Center (FMC)
- Cisco Firepower Threat Defense (FTD)
- Cisco Identity Services Engine (ISE) versions 3.0.x antérieures à 3.0P8
- Cisco Identity Services Engine (ISE) versions 3.1.x antérieures à 3.1P8
- Cisco Identity Services Engine (ISE) versions 3.2.x antérieures à 3.2P3
- Cisco Identity Services Engine (ISE) versions antérieures à 2.7P10

DÉSCRIPTION :

Plusieurs vulnérabilités de haute importance ont été résolues dans les produits Cisco mentionnés. Ces vulnérabilités pourraient être utilisées par un attaquant pour provoquer un déni de service, exécuter du code à distance de manière non autorisée, obtenir une élévation de privilèges, ou contourner les politiques de sécurité.

SOLUTION :

- Se référer au bulletin de sécurité Cisco du 01 Novembre 2023 pour plus d'information(Documentation).

DOCUMENTATION :

- Bulletins de sécurité Cisco du 01 Novembre 2023:

https://sec.cloudapps.cisco.com/security/center/content/ciscosecurityadvisory/cisco-safmc-cmd-inj-29mp49hn

https://sec.cloudapps.cisco.com/security/center/content/ciscosecurityadvisory/cisco-saasa-icmpv6-t5tzqwnd

https://sec.cloudapps.cisco.com/security/center/content/ciscosecurityadvisory/cisco-saasa-webvpn-dos-3ghzqbas

https://sec.cloudapps.cisco.com/security/center/content/ciscosecurityadvisory/cisco-safmc-cmdinj-btegufox

https://sec.cloudapps.cisco.com/security/center/content/ciscosecurityadvisory/cisco-safmc-logview-dos-ayjdex55

https://sec.cloudapps.cisco.com/security/center/content/ciscosecurityadvisory/cisco-saftd-fmc-code-inj-wshrgz8l

https://sec.cloudapps.cisco.com/security/center/content/ciscosecurityadvisory/cisco-saftd-icmpv6-dos-4emklun

https://sec.cloudapps.cisco.com/security/center/content/ciscosecurityadvisory/cisco-saftd-intrusion-dos-dft7wygc

https://sec.cloudapps.cisco.com/security/center/content/ciscosecurityadvisory/cisco-saise-file-upload-fcelp4xs

- CVE-2023-20048

https://nvd.nist.gov/vuln/detail/CVE-2023-20048

- CVE-2023-20063

https://nvd.nist.gov/vuln/detail/CVE-2023-20063

- CVE-2023-20083

https://nvd.nist.gov/vuln/detail/CVE-2023-20083

- CVE-2023-20086

https://nvd.nist.gov/vuln/detail/CVE-2023-20086

- CVE-2023- 20095

https://nvd.nist.gov/vuln/detail/CVE-2023-20095

- CVE-2023-20155

https://nvd.nist.gov/vuln/detail/CVE-2023-20155

- CVE-2023-20170

https://nvd.nist.gov/vuln/detail/CVE-2023-20170

- CVE-2023-20175

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20175

- CVE-2023-20195

https://nvd.nist.gov/vuln/detail/CVE-2023-20195

- CVE2023-20196

https://nvd.nist.gov/vuln/detail/CVE-2023-20196

- CVE-2023-20213

https://nvd.nist.gov/vuln/detail/CVE-2023-20213

- CVE-2023-20219

https://nvd.nist.gov/vuln/detail/CVE-2023-20219

- CVE-2023-20220

https://nvd.nist.gov/vuln/detail/CVE-2023-20220

- CVE-2023-20244

https://nvd.nist.gov/vuln/detail/CVE-2023-20244