Centre de Veille de Détection et
de Réaction aux Attaques
Informatiques

مركز اليقظة والرصد
والتصدي للهجمات المعلوماتية

Bulletin de sécurité du maCERT

Titre: Vulnérabilités corrigées dans de multiples produits de Cisco

Numéro de Référence : 21532208/19
Risque : Important
Impact : Important

Systèmes affectés

- Cisco Integrated Management Controller Supervisor versions antérieures à 2.2.1.0
- Cisco UCS Director versions 6.5 et 6.6
- Cisco UCS Director versions antérieures à 6.7.3.0
- Cisco UCS Director Express for Big Data versions antérieures à 3.7.3.0
- Cisco IMC versions 1.5(x) antérieures à 1.5(9g) sur UCS séries C et S
- Cisco IMC versions 2.0(x) antérieures à 2.0(13o) sur UCS séries C et S
- Cisco IMC versions 3.0(x) antérieures à 3.0(4k) sur UCS séries C et S
- Cisco IMC versions 4.0(x) antérieures à 4.0(1d), 4.0(2c), 4.0(2f) et 4.0(4b) sur UCS séries C et S

Identificateurs externes

CVE-2019-1938, CVE-2019-1935, CVE-2019-1974, CVE-2019-1937, CVE-2019-12634, CVE-2019-1885, CVE-2019-1863, CVE-2019-1907, CVE-2019-1908, CVE-2019-1900 CVE-2019-1896, CVE-2019-1634, CVE-2019-1865, CVE-2019-1864, CVE-2019-1850, CVE-2019-1883

Bilan de la vulnérabilité

Cisco annonce la correction de plusieurs vulnérabilités dans certains de ses produits. L'exploitation de ces vulnérabilités peut permettre à un attaquant distant d'exécuter du code arbitraire, provoquer un déni de service ou de contourner la politique de sécurité.

Solution

Veuillez-vous référer aux bulletins de sécurité de Cisco :

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-ucsd-

authbypass
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imcs-usercred
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imcs-ucs-authbypass

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imcs-ucs-authby
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-ucs-imc-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-ucs-cimc
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imcs-ucs-cmdinj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-privilege
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-privescal
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-infodisc
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-dos

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-cmdinject-1896
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-cmdinject-1634

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-cmdinj-1865
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-cmdinj-1864
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-cmdinj-1850
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-bo
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-cimc-cli-inject

Risque :

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

Annexe

Bulletins de sécurité de Cisco :

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-ucsd-authbypass
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imcs-usercred
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imcs-ucs-authbypass

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imcs-ucs-authby
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-ucs-imc-dos
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-ucs-cimc
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imcs-ucs-cmdinj
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-privilege
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-privescal
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-infodisc
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-dos

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-cmdinject-1896
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-cmdinject-1634

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-cmdinj-1865
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-cmdinj-1864
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-cmdinj-1850
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-imc-bo
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190821-cimc-cli-inject

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات, مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma