Computer Emergency Response Team

BOLLETTINO IT-CERT.180621.B01

Vulnerabilità critiche in Cisco FXOS e NX-OS

(CVE-2018-0301, CVE-2018-0308, CVE-2018-0304, CVE-2018-0314, CVE-2018-0312)

MINISTERO DELLO
SVILUPPO ECONOMICO

DESCRIZIONE

Cisco FXOS è un sistema operativo che equipaggia i firewall di nuova generazione della famiglia Firepower prodotti da Cisco Systems. **Cisco NX-OS** è un sistema operativo di rete espandibile, aperto e programmabile che consente di gestire e programmare *switch* attraverso opportune API.

Sono state scoperte numerose vulnerabilità, di cui cinque critiche, nei prodotti software **Cisco FXOS** e **Cisco NX-OS**. Queste vulnerabilità possono essere sfruttate da un attaccante remoto non autenticato per provocare il *crash* di un sistema affetto, con conseguente condizione di *denial of service* (DoS), o potenziale esecuzione di codice arbitrario con privilegi elevati.

Si riportano per informazione brevi descrizioni delle vulnerabilità, con i rispettivi codici CVE:

- **[Critical] CVE-2018-0301**: una vulnerabilità nella funzionalità NX-API di Cisco NX-OS potrebbe consentire ad un attaccante remoto non autenticato di causare un *buffer overflow* mediante invio di un pacchetto appositamente predisposto all'interfaccia di gestione di un sistema affetto.
- **[Critical] CVE-2018-0308**: una vulnerabilità nel componente Cisco Fabric Services (CFS) di Cisco FXOS e di Cisco NX-OS potrebbe consentire a un attaccante remoto non autenticato di eseguire codice arbitrario o causare una condizione di DoS.
- **[Critical] CVE-2018-0304**: una vulnerabilità nel componente CFS di Cisco FXOS e di Cisco NX-OS potrebbe consentire a un attaccante remoto non autenticato di accedere al contenuto della memoria, causare una condizione di DoS o eseguire codice arbitrario come *root*.
- **[Critical] CVE-2018-0314**: una vulnerabilità nel componente CFS di Cisco FXOS e di Cisco NX-OS potrebbe consentire a un attaccante remoto non autenticato di eseguire codice arbitrario su un dispositivo affetto.
- **[Critical] CVE-2018-0312**: una vulnerabilità nel componente CFS di Cisco FXOS e di Cisco NX-OS potrebbe consentire a un attaccante remoto non autenticato di eseguire codice arbitrario o causare una condizione di DoS su un dispositivo affetto.

Al momento non ci sono notizie che queste vulnerabilità siano state sfruttate in attacchi reali.

Cisco ha rilasciato aggiornamenti software che risolvono queste ed altre vulnerabilità di gravità elevata nei prodotti interessati. Non sono disponibili soluzioni alternative per mitigare queste vulnerabilità (per maggiori informazioni si veda la sezione LINK UTILI).

SOLUZIONE

I gestori di dispositivi equipaggiati con i sistemi Cisco FXOS e Cisco NX-OS devono verificare la versione del sistema installato sui propri dispositivi mediante la linea di comando (CLI) o l'interfaccia di amministrazione e controllare che non risulti affetta da una o più delle vulnerabilità descritte nel presente bollettino.

In caso di riscontro positivo, si raccomanda di installare al più presto gli aggiornamenti relativi alla propria piattaforma.

Per maggiori informazioni sui prodotti vulnerabili e sugli aggiornamenti disponibili si raccomanda di consultare i relativi bollettini di sicurezza di Cisco (si veda la sezione LINK UTILI).

SISTEMI

Le vulnerabilità oggetto di questo bollettino affliggono diverse versioni di Cisco FXOS e Cisco NX-OS installate sulle famiglie di dispositivi Cisco di seguito elencate:

- Firepower 4100 Series Next-Generation Firewalls
- Firepower 9300 Security Appliance
- MDS 9000 Series Multilayer Switches
- Nexus 2000 Series Fabric Extenders
- Nexus 3000 Series Switches
- Nexus 3500 Platform Switches
- Nexus 5500 Platform Switches
- Nexus 5600 Platform Switches
- Nexus 6000 Series Switches
- Nexus 7000 Series Switches
- Nexus 7700 Series Switches
- Nexus 9000 Series Switches in standalone NX-OS mode
- Nexus 9500 R-Series Line Cards and Fabric Modules
- UCS 6100 Series Fabric Interconnects
- UCS 6200 Series Fabric Interconnects
- UCS 6300 Series Fabric Interconnects

Le versioni vulnerabili dei sistemi Cisco FXOS e Cisco NX-OS sono indicate per ognuna delle famiglie di dispositivi coinvolti nelle tabelle incluse nei relativi bollettini di sicurezza di Cisco (si veda la sezione LINK UTILI).

LINK UTILI

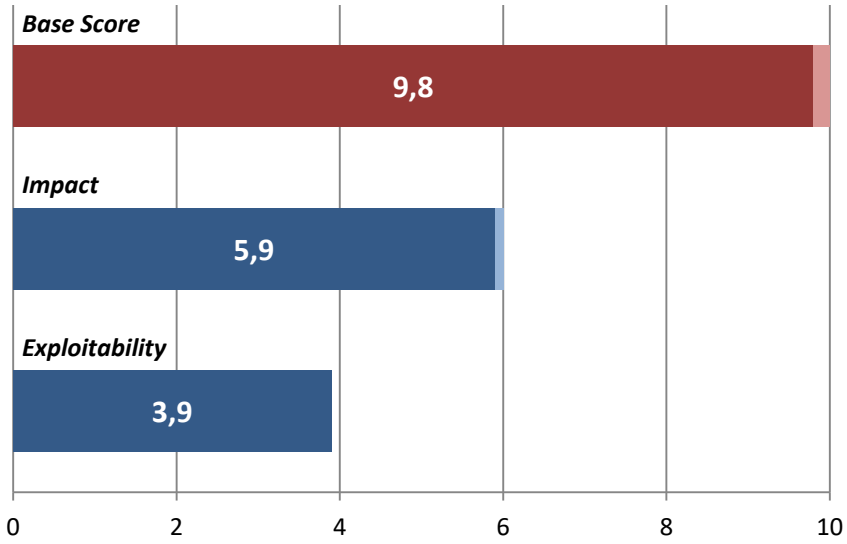
Avvisi del produttore

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180620-nxos-bo
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180620-fxnxos-fab-ace
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180620-fxnxos-ace
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180620-fx-os-fabric-execution
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180620-fx-os-cli-execution

Mitre CVE ID

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0301
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0308
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0304
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0314
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0312

VALUTAZIONE CVSS



Relativamente alla valutazione della *severity* come metrica di base - da intendersi quale livello di pericolosità della vulnerabilità delle componenti di sistema o delle piattaforme - il CERT Nazionale valuta i parametri che concorrono al calcolo della *Base Score* secondo lo standard CVSS v3 (*Common Vulnerabilities Scoring System*), avvalendosi del *tool* messo a disposizione dal sito del NIST (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator).

Nello specifico, per tutte le vulnerabilità oggetto del presente bollettino, sono stati raggiunti i seguenti punteggi:

- *Base Score:* 9,8
- *Impact:* 5,9
- *Exploitability:* 3,9

Vettore CVSS: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

NOTE

Le informazioni contenute nel presente bollettino sono fornite a meri fini informativi.

In nessun caso il CERT Nazionale può essere ritenuto responsabile di qualunque perdita, pregiudizio, responsabilità, costo, onere o spesa, ivi comprese le eventuali spese legali, danno diretto, indiretto, incidentale o consequenziale, derivante da o connesso alle informazioni riportate nel presente bollettino.

La versione PDF del bollettino è statica ed, in quanto tale, contiene le informazioni disponibili al momento della pubblicazione.