# Security Advisory: Proietti Planet Time Enterprise (CVE-2022-30422)


L'Offensive Security Team di Swascan ha identificato una vulnerabilità della web app **Proietti Planet Time Enterprise**.

# Proietti T

**Proietti Tech Sr**
apparecchiatur
e raccolta dati).

## Descrizio

Planet Time En
Proietti.

Un potente stru
dei processi e l
tempo reale.

La possibilità d
configurazione
che per realtà p

Il Planet Time E
di gestire tutti
risorse umane.



## Technical summary

Il Cyber Security Team di Swascan ha trovato un importante vulnerabilità su: Planet Time Enterprise Web

| Assets | Vulnerability | CVSS | Severity |
|---|---|---|---|
| | | | |

Planet Time En
4 .0.1, 4.2.0.0, 4
3.0.0

Nella seguente
comprese le ev
centinaia di clie

## Descrizio

L'applicazione r
default.

Un potenziale a
dall'applicativo,
deserialization
diretto alla mac

Per sfruttare co
autenticazione.

Di seguito vien
remoto sfruttando la vulnerabilità.



## Proof of Concept

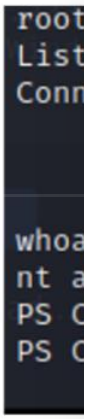
Di seguito viene riportato il comando utilizzato per generare il payload che ha consentito di eseguire comandi da remoto attraverso una POST request come parametro VIEWSTATE:

```
.\ysoserial.
"powershell
JABjAG-wAaQE
snipped..UAb
validational
generator=..
```

Dopo aver gene
creato sopra.


Evidenza 1 – Richiesta POST

Dopo aver inviato la POST request il risultato del payload è una shell interattiva sul server che ospita l'applicativo.



## Impatto

L'attaccante pu
windows, come
laterali ed encr

## Remediat

- Assicurarsi ch
vendor.
- Verificare che le seguenti impostazioni siano configurate per IIS:

  – enableViewStateMac sia impostata su 'true'
  – aspnet:AllowInsecureDeserialization sia impostata su 'false'

- Rigenerare o sostituire le chiavi di convalida nel file web.config o impostare la generazione automatica delle stesse.
- Aggiornare il software all'ultima versione disponibile.

## Riferimen

- https://owasp
- https://cwe.n
- https://dotne
- https://sorou

net-via-viewsta

- https://githul
- https://www.

## Disclosur

- 29-03-2022: V
- 07-04-2022: V
- 21-04-2022: V
- 22-04-2022: C
- 03-05-2022: C
- 19-05-2022: V
- 27-05-2022: C
- 31-05-2022: accordo per la data di pubblicazione del security advisory
- 16-06-2022: pubblicazione del security advisory




Swascan Academy lancia la Seconda Edizione del corso propedeutico alla Certificazione CISSP!

Chrome Loader: Analisi Malware

Iscriviti al

La newsletter di Sw

Cyber per restare s

EMAIL

Il sottoscritto, dichia
l'attivazione del serv

# Pronto intervento Cyber Swascan

Contattaci per un supporto immediato

NOME*

COGNOME*

TELEFONO*

EMAIL*

MESSAGGIO*

Il sottoscritto, in qualità di interessato DICHIARA di aver letto e compreso il contenuto della privacy policy ai sensi dell'articolo 13, GDPR. ACCONSENTE al trattamento dei Dati in relazione all'invio da parte del Titolare di comunicazioni commerciali e/o promozionali relative a (i) prodotti/servizi propri, ovvero a (ii) prodotti/servizi offerti da terze parti.
Il consenso prestato potrà essere revocato in qualsiasi momento contattando il Titolare ai recapiti presenti nella citata privacy policy.

# Pronto intervento Cyber Swascan

Contattaci per un supporto immediato

NOME*

COGNOME*

TELEFONO*

EMAIL*

MESSAGGIO*

☐ Il sottoscritto, in qualità di interessato DICHIARA di aver letto e compreso il contenuto della privacy policy ai sensi dell'articolo 13, GDPR. ACCONSENTE al trattamento dei Dati in relazione all'invio da parte del Titolare di comunicazioni commerciali e/o promozionali relative a (i) prodotti/servizi propri, ovvero a (ii) prodotti/servizi offerti da terze parti.
Il consenso prestato potrà essere revocato in qualsiasi momento contattando il Titolare ai recapiti presenti nella citata privacy policy.