

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°141			Fecha: 16-06-2023						
				Página: 4 de 11						
Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL									
Nombre de la alerta	Escalada de privilegios en productos Pulse Secure									
Tipo de Ataque	Abuso de privilegios o de políticas de seguridad	Abreviatura	AbuPrivPolSeg							
Medios de propagación	Red, Internet									
Código de familia	K	Código de Sub familia	K01							
Clasificación temática familia	Uso inapropiado de recursos									
Descripción										
<p>1. ANTECEDENTES</p> <ul style="list-style-type: none"> Siris es una firma de capital privado que invierte en negocios de tecnología y telecomunicaciones. En el año 2014 adquiere el negocio Junos Pulse de Juniper Networks y funda una entidad independiente llamada Pulse Secure. La compañía Pulse Secure adquiere ese mismo año a MobileSpaces un proveedor líder de seguridad móvil. Pulse Secure fue adquirida por Ivanti el 01 de diciembre de 2020. Los Investigadores independientes notificaron al proveedor el 27/07/22 sobre una vulnerabilidad de día cero, con esta información el proveedor tiene la oportunidad de implementar un parche y lanzarlo a sus clientes, de acuerdo con su política de divulgación cuando el parche esté listo se hará pública la vulnerabilidad de día cero. Los investigadores independientes solicitan una actualización e informan al proveedor que el caso se publicará como un aviso de día cero el 14/06/23. <p>2. DETALLES:</p> <p>El proceso de escalamiento de privilegios locales es el siguiente: El ciberdelincuente primero debe obtener la capacidad de ejecutar código con pocos privilegios en el sistema de destino para aprovechar esta vulnerabilidad. El problema se debe a la falta de validación adecuada de una ruta proporcionada por el usuario antes de usarla en las operaciones con archivos. El ciberdelincuente puede aprovechar esta vulnerabilidad para aumentar los privilegios y ejecutar código arbitrario en el contexto del servidor.</p> <p>A. Indicadores de Compromiso</p> <ul style="list-style-type: none"> Se ha asignado el siguiente identificador para esta vulnerabilidad: <table border="1" style="margin-left: 40px;"> <thead> <tr> <th>ZDI ID</th> <th>CVE ID</th> <th>Puntuación CVSS</th> </tr> </thead> <tbody> <tr> <td>ZDI-23-858 ZDI-CAN-17687</td> <td>CVE-2023-34298</td> <td>Alta (7.8)</td> </tr> </tbody> </table> <p>A pesar que el proveedor fue notificado hace apropiadamente 11 meses de esta vulnerabilidad de día cero de escalamiento de privilegios locales esto fue ignorado en su informe mensual. Al no haber un parche oficial y contar con tiempo para implementar el parche hace que la vulnerabilidad de día cero sea considerada no crítica y con puntuación 7.8 al no existir una solución.</p> <p>B. Productos afectados</p> <ul style="list-style-type: none"> Pulse Secure Client SetupService Directory Traversal Local. <p>3. RECOMENDACIONES:</p> <ul style="list-style-type: none"> Evitar interactuar la aplicación y reportar a su soporte de seguridad informática o mesa de ayuda. 					ZDI ID	CVE ID	Puntuación CVSS	ZDI-23-858 ZDI-CAN-17687	CVE-2023-34298	Alta (7.8)
ZDI ID	CVE ID	Puntuación CVSS								
ZDI-23-858 ZDI-CAN-17687	CVE-2023-34298	Alta (7.8)								
Fuente de Información:	<ul style="list-style-type: none"> hxxps://www.cve.org/CVERecord?id=CVE-2023-30743 hxxps://www.zerodayinitiative.com/advisories/ZDI-23-858/ hxxps://www.ivanti.com/blog/june-2023-patch-Tuesday hxxps://www.ivanti.com/blog/june-2023-patch-tuesday 									